

# Quantum Information Complexity and Amortized Communication

Dave Touchette<sup>1</sup>

## Abstract

We define a new notion of information cost for quantum protocols, and a corresponding notion of quantum information complexity for bipartite quantum channels, and then investigate the properties of such quantities. These are the fully quantum generalizations of the analogous quantities for bipartite classical functions that have found many applications recently, in particular for proving communication complexity lower bounds. Our definition is strongly tied to the quantum state redistribution task.

Previous attempts have been made to define such a quantity for quantum protocols, with particular applications in mind; our notion differs from these in many respects. First, it directly provides a lower bound on the quantum communication cost, independent of the number of rounds of the underlying protocol. Secondly, we provide an operational interpretation for quantum information complexity: we show that it is exactly equal to the amortized quantum communication complexity of a bipartite channel on a given state. This generalizes a result of Braverman and Rao to quantum protocols, and even strengthens the classical result in a bounded round scenario. Also, this provides an analogue of the Schumacher source compression theorem for interactive quantum protocols, and answers a question raised by Braverman.

We also discuss some potential applications to quantum communication complexity lower bounds by specializing our definition for classical functions and inputs. Building on work of Jain, Radhakrishnan and Sen, we provide new evidence suggesting that the bounded round quantum communication complexity of the disjointness function is  $\Omega(\frac{n}{M} + M)$ , for  $M$ -message protocols. This would match the best known upper bound.

---

<sup>1</sup>touchette.dave@gmail.com, Laboratoire d'informatique théorique et quantique, Département d'informatique et de recherche opérationnelle, Université de Montréal.

# 1 Introduction

The paradigm of information complexity has been quite successful recently in classical communication complexity. What started out as a useful tool for proving communication complexity lower bounds has recently developed into an important subfield of its own. The definition of information complexity, the sum of the mutual information between the protocol transcript and each player's input conditional on the other player's input, makes it possible to bring powerful tools from information theory to study interactive communication. Many recent results show that this paradigm has enabled researchers to tackle questions that seemed out of reach not so long ago, like an exact characterization by Braverman, Garg, Pankratov, and Weinstein [17] of the communication complexity of the disjointness function.

The first results on information complexity were those of Chakrabarti, Shi, Wirth and Yao [22], who gave lower bounds for communication complexity in the simultaneous message passing model by defining what would now be called external information cost. A subsequent paper by Bar-Yossef, Jayram, Kumar and Sivakumar [4] implicitly defined what is now called the internal information cost, or simply information cost. They used it to prove communication complexity lower bounds for functions that can be built from simpler component functions, like the set disjointness function with respect to the AND function. The recent wave of results started with a compression result of Barak, Braverman, Chen and Rao [5] that had application in particular to proving a direct sum theorem for randomized communication complexity. In [19], Braverman and Rao give an exact operational interpretation of the information complexity as the amortized distributional communication complexity, which can be viewed as an analogue of the Shannon source compression theorem for interactive protocols. In [14], Braverman provides a prior-free definition for information complexity of classical functions, and presents a similar operational interpretation for worst case amortized communication complexity. Since then, many results have been derived by using the information complexity paradigm [17, 18, 16], witnessing its power. Braverman provides a nice overview of results circa 2012 [15].

It might appear surprising that the definition of this simple looking quantity, the information cost of a protocol, has such far reaching consequences. It is tempting to try to bring such a paradigm to the quantum setting and hopefully get comparable results. However, there are many difficulties in trying to get such a quantum generalization of information cost. Firstly, due to monogamy of entanglement, there is no good notion of an overall transcript and its corresponding correlation with the localized inputs at the beginning of the protocol. Indeed, it is only possible to evaluate quantum information quantities for quantum registers that are defined at the same moment in time. But then, the no-cloning theorem [25, 35] forbids copying of previous messages to generate a final transcript accounting for all communication in the quantum protocol, on which we could evaluate a quantum information cost. Even for protocols with pre-shared entanglement and classical communication, the final classical transcript could be completely uncorrelated to the inputs. This can be seen for example in a protocol that teleports at each time step, which would generate a transcript that is uniformly distributed. However, notwithstanding these difficulties, Jain, Radhakrishnan and Sen [27], as well as Jain and Nayak [26], gave different definitions for such a quantity with specific applications in mind. In particular, the definition in [27] leads to a beautiful proof of a lower bound of  $\Omega(\frac{n}{M^2} + M)$  on bounded round quantum communication complexity for (size  $n$ )

set disjointness computed by  $M$ -message protocols. Note that the remark is made in [27] that the optimal  $\Theta(\sqrt{n})$  protocol of Aaronson and Ambainis [1] can be adapted to yield a bounded round protocol achieving communication of  $O(\frac{n}{M} + M)$ . Hence, this comes close to match the best known upper bound. However, even if these definitions can be successful for obtaining interesting results in a bounded round scenario, it is quite plausible that they are also limited to such applications. Indeed, given these previous definitions of quantum information cost, it is quite easy to find particular inputs and protocols with  $M$  messages and quantum communication cost  $C$  such that the quantum information cost is  $\Omega(M \cdot C)$ . We believe that a more natural definition of quantum information cost would not have such a dependence on the round complexity of protocols. In contrast, the classical information cost directly provides a lower bound on the communication cost, and this property is crucial in many of its recent applications. Hopefully, it would also lead to an operational interpretation analogous to the classical one for amortized quantum communication complexity. A related question was asked by Braverman [14], on how to define the correct quantum analogue of information complexity.

## 2 Overview of Results

We show that despite the previously mentioned setbacks, it is possible to define a quantum information cost quantity for protocols and a corresponding quantum information complexity quantity for channels that satisfies the two important properties asked for above. First, they are lower bounds on the quantum communication cost and quantum communication complexity of the corresponding protocols and channels, respectively. Secondly, we can compress asymptotically any protocol to its quantum information cost, and so we can give the operational interpretation for quantum information complexity as the amortized quantum communication complexity. That is, the quantum communication complexity per copy for implementing  $n$  copies of the channel, in the asymptotic limit of large  $n$ . The quantity that we consider would be the fully quantum analogue of the distributional information complexity of functions: we study the quantum information complexity of a channel on some arbitrary quantum input. In the case of a so-called classical input, this corresponds to a probability distribution. When implementing a bipartite channel with a protocol on a general input, we allow for some small error  $\varepsilon$  in the trace distance with respect to a reference system purifying the input. The introduction of the reference system is to ensure that our implementation maintains correlations with the outside world as well as the actual channel. For classical inputs and functions, we show that this implies a bound on the probability of failure, in the sense of a classical average on the input distribution, of the quantum protocol for computing the function. Hence, this links our quantity to the distributional quantum communication complexity of classical functions. When implementing  $n$  copies of a general channel, the success criterion is that for each instance of the channel, the error is bounded by  $\varepsilon$ .

To circumvent the difficulties we mentioned in defining a quantum generalization of information cost and complexity, we take a different perspective on the classical definitions. Indeed, our main insight in defining such quantities comes by using a rewriting of the information cost of a protocol that was already implicit in previous works on information

complexity. We reinterpret this quantity by viewing each message generation in the protocol as a noisy channel whose output is to be sent over a noiseless channel. Then, message transmission is viewed as the simulation, over a noiseless channel, of a noisy channel with feedback to the sender and side information at the receiver. This is a variant of what is known as a (tensor power input) classical reverse Shannon theorem in the information theory literature. Using previously known results [9, 31], we obtain an alternate, simple proof of the operational interpretation of classical information complexity. An additional feature of this proof in contrast to the one of Braverman and Rao [19] is that it maintains the round complexity of the original protocol, since these results about noisy channel simulation use only unidirectional transmission. To the best of our knowledge, this is the first proof to establish that the  $M$ -message information complexity is exactly equal to the  $M$ -message amortized communication complexity. Note however that this proof only works in the asymptotic limit, so we do not get as a bonus of the techniques used for our coding theorem a compression theorem for a single copy of the protocol. It is reasonable to hope that eventual results on so-called one-shot unidirectional coding theorems might lead to interesting results about bounded round, single copy protocol compression.

Using this perspective on classical information cost, we can more easily define a quantum generalization. The right quantum analogue of the reverse Shannon task with feedback and side information is quantum state redistribution, for which Devetak and Yard give an optimal protocol [24, 37]. With these tools in hands, we then define the quantum analogues of information cost and complexity, and prove their operational interpretations. In addition, we also prove some interesting properties of these quantities. In particular, it is an almost immediate consequence of the definition that the quantum information cost of a protocol lower bounds its quantum communication cost, and then a similar result holds for quantum communication complexity relative to channels. We also prove that with our definition, the quantum information complexity is an additive quantity, and that it is convex and continuous in the channel and error parameter. Finally, relative to input states, we prove a concavity result on quantum information cost. At this point, given this operational interpretation and the fact that information is a lower bound on communication, we might argue that this corresponds to the right quantum analogue of the information complexity.

To demonstrate the potential of the quantum information complexity paradigm, we reduce the quantum information complexity of the disjointness function to that of the AND function, a reduction along similar lines as that of [4, 27]. In contrast to the quantum reduction of [27], we are able to get rid of a factor  $\frac{1}{M}$  for quantum protocols with  $M$  messages. Given that their lower bound for bounded round complexity for  $n$ -bit disjointness is  $\Omega(\max(\frac{n}{M^2}, M))$ , we are thus optimistic that this reduction by a factor of  $\frac{1}{M}$  using our approach could lead to a lower bound of  $\Omega(\max(\frac{n}{M}, M))$ , thus matching the best currently known upper bound [1, 27]. Like classical information cost, our quantity is defined in terms of conditional mutual information, a quantity that has been notoriously hard to lower bound in the quantum setting [30, 13]. We leave as an interesting open problem to develop tools for lower bounding the conditional mutual information in our setting, and to see if we can obtain such a result for the disjointness function. We explore other potential applications in the conclusion.

**Organization.** The structure of the paper is the following. In the next section, we fix the notation that we use for quantum mechanics, present the necessary quantum information theory background, define formally the quantum communication model that we use and also define quantum communication complexity in this model. We then present a perspective on classical information complexity that leads us to a quantum generalization, then give such a definition of quantum information complexity and finally prove its operational interpretation in the following section. We also explore some of the properties of our definition, and then go on to discuss some potential applications. We conclude with a discussion of our results, additional potential applications, and further research directions.

## 3 Preliminaries

### 3.1 Quantum Information Theory

We use the following notation for quantum theory; see [33, 34] for more details. We associate a quantum register  $A$  with a corresponding vector space, also denoted by  $A$ . We only consider finite-dimensional vector spaces. A state of quantum register  $A$  is represented by a density operator  $\rho \in \mathcal{D}(A)$ , with  $\mathcal{D}(A)$  the set of all unit trace, positive semi-definite linear operators mapping  $A$  into itself. We say that a state  $\rho$  is pure if it is a projection operator, i.e.  $(\rho^{AR})^2 = \rho^{AR}$ . For a pure state  $\rho$ , we often use the pure state formalism, and represent  $\rho$  by the vector  $|\rho\rangle$  it projects upon, i.e.  $\rho = |\rho\rangle\langle\rho|$ . A quantum channel from quantum register  $A$  into quantum register  $B$  is represented by a super-operator  $\mathcal{N}^{A \rightarrow B} \in \mathcal{C}(A, B)$ , with  $\mathcal{C}(A, B)$  the set of all completely positive, trace-preserving linear operators from  $\mathcal{D}(A)$  into  $\mathcal{D}(B)$ . If  $A = B$ , we might simply write  $\mathcal{N}^A$ , and when systems are clear from context, we might drop the superscripts. For channels  $\mathcal{N}_1 \in \mathcal{C}(A, B), \mathcal{N}_2 \in \mathcal{C}(B, C)$  and state  $\rho \in \mathcal{D}(A)$ , we denote their composition as  $\mathcal{N}_2 \circ \mathcal{N}_1 \in \mathcal{C}(A, C)$ , with action  $\mathcal{N}_2 \circ \mathcal{N}_1(\rho) = \mathcal{N}_2(\mathcal{N}_1(\rho))$ . We might drop the  $\circ$  if the composition is clear from context. For  $A$  and  $B$  isomorphic, we denote the identity mapping as  $I^{A \rightarrow B}$ , with some implicit choice for the change of basis. For  $\mathcal{N}^{A_1 \rightarrow B_1} \otimes I^{A_2 \rightarrow B_2} \in \mathcal{C}(A_1 \otimes A_2, B_1 \otimes B_2)$ , we might abbreviate this as  $\mathcal{N}$  and leave the identity channel implicit when the meaning is clear from context. An important subset of  $\mathcal{C}(A, B)$  when  $A$  and  $B$  are isomorphic spaces is the set of unitary channels  $\mathcal{U}(A, B)$ , the set of all maps  $U \in \mathcal{C}(A, B)$  with an adjoint map  $U^\dagger \in \mathcal{C}(B, A)$  such that  $U^\dagger \circ U = I^A$ . Another important example of channel that we use is the partial trace  $\text{Tr}_B(\cdot) \in \mathcal{C}(A \otimes B, A)$  which effectively gets rid of the  $B$  subsystem. Fixing a basis  $\{|b\rangle\}$  for  $B$ , the action of  $\text{Tr}_B$  on any  $\rho^{AB} \in \mathcal{D}(A \otimes B)$  is  $\text{Tr}_B(\rho^{AB}) = \sum_b \langle b | \rho^{AB} | b \rangle$ , and we write  $\rho^A = \text{Tr}_B(\rho^{AB})$ . We also denote  $\text{Tr}_{-A} = \text{Tr}_B$  to express that we want to keep only the  $A$  register. Fixing a basis also allows us to talk about classical states and joint states:  $\rho \in \mathcal{D}(B)$  is classical (with respect to this basis) if it is diagonal in basis  $\{|b\rangle\}$ , i.e.  $\rho = \sum_b p_B(b) |b\rangle\langle b|$  for some probability distribution  $p_B$ . More generally, subsystem  $B$  of  $\rho^{AB}$  is said to be classical if we can write  $\rho^{AB} = \sum_b p_B(b) |b\rangle\langle b|^B \otimes \rho_b^A$  for some  $\rho_b^A \in \mathcal{D}(A)$ . An important example of a channel mapping a quantum system to a classical one is the measurement channel  $\Delta_B$ , defined as  $\Delta_B(\rho) = \sum_b \langle b | \rho | b \rangle \cdot |b\rangle\langle b|^B$  for any  $\rho \in \mathcal{D}(B)$ . Often,  $A, B, C, \dots$  will be used to discuss general systems, while  $X, Y, Z, \dots$  will be reserved for classical systems. For a state  $\rho^A \in \mathcal{D}(A)$ , a purification is a pure state  $\rho^{AR} \in \mathcal{D}(A \otimes R)$  satisfying  $\text{Tr}_R(\rho^{AR}) = \rho^A$ .

If  $R$  has dimension at least that of  $A$ , then such a purification always exists. For a given  $R$ , all purifications are equivalent up to unitaries. For a channel  $\mathcal{N} \in C(A, B)$ , a unitary extension is a unitary  $U_{\mathcal{N}} \in U(A \otimes B', A' \otimes B)$  with  $\text{Tr}_{A'}(U_{\mathcal{N}}(\rho^A \otimes \sigma^{B'})) = \mathcal{N}(\rho^A)$  for some fixed  $\sigma \in \mathcal{D}(B')$ . It is sufficient to consider any fixed pure state  $\sigma$ . Such an extension always exists provided  $A'$  is of dimension at least  $\dim(A)^2$  (note that we also must have  $\dim(A) \cdot \dim(B') = \dim(A') \cdot \dim(B)$ ).

The notion of distance we use is the trace distance, defined for two states  $\rho_1, \rho_2 \in D(A)$  as the sum of the absolute values of the eigenvalues of their difference:

$$\|\rho_1 - \rho_2\|_A = \text{Tr}(|\rho_1 - \rho_2|).$$

It has an operational interpretation as four times the best bias possible in a state discrimination test between  $\rho_1$  and  $\rho_2$ . The subscript tells on which subsystems the trace distance is evaluated, and remaining subsystems might need to be traced out. We use the following results about trace distance. For proofs of these and other standard results in quantum information theory that we use, see [34]. The trace distance is monotone under noisy channels: for any  $\rho_1, \rho_2 \in \mathcal{D}(A)$  and  $\mathcal{N} \in C(A, B)$ ,

$$\|\mathcal{N}(\rho_1) - \mathcal{N}(\rho_2)\|_B \leq \|\rho_1 - \rho_2\|_A. \quad (3.1)$$

For unitaries, the equality becomes an identity, a property called unitary invariance of the trace distance. Hence, for any  $\rho_1, \rho_2 \in D(A)$  and any  $U \in \mathcal{U}(A, B)$ , we have

$$\|U(\rho_1) - U(\rho_2)\|_B = \|\rho_1 - \rho_2\|_A. \quad (3.2)$$

Also, the trace distance cannot be increased by adjoining an uncorrelated system: for any  $\rho_1, \rho_2 \in D(A), \sigma \in \mathcal{D}(B)$

$$\|\rho_1 \otimes \sigma - \rho_2 \otimes \sigma\|_{AB} = \|\rho_1 - \rho_2\|_A. \quad (3.3)$$

It follows that the trace distance obeys a property that we call joint linearity: for a classical system  $X$  and two states  $\rho_1^{XA} = p_X(x)|x\rangle\langle x|^X \otimes \rho_{1,x}^A, \rho_2^{XA} = p_X(x)|x\rangle\langle x|^X \otimes \rho_{2,x}^A$ ,

$$\|\rho_1 - \rho_2\|_{XA} = \sum_x p_X(x) \|\rho_{1,x} - \rho_{2,x}\|_A. \quad (3.4)$$

The measure of information that we use is the von Neumann entropy, defined for any state  $\rho \in D(A)$  as

$$H(A)_\rho = \text{Tr}(\rho \log \rho),$$

in which we take the convention that  $0 \log 0 = 0$ , justified by a continuity argument. All logarithms are taken base 2. Note that  $H$  is invariant under unitaries applied on  $\rho$ . If the state to be evaluated is clear from context, we might drop the subscript. Conditional entropy for a state  $\rho^{ABC} \in D(A \otimes B \otimes C)$  is then defined as

$$H(A|B)_{\rho^{AB}} = H(AB)_{\rho^{AB}} - H(B)_{\rho^B},$$

mutual information as

$$I(A; B)_{\rho^{AB}} = H(A)_{\rho^A} - H(A|B)_{\rho^{AB}},$$

and conditional mutual information as

$$I(A; B|C)_{\rho^{ABC}} = H(A|C)_{\rho^{AC}} - H(A|BC)_{\rho^{ABC}}.$$

Note that mutual information and conditional mutual information are symmetric in interchange of  $A, B$ . For any pure bipartite state  $\rho^{AB} \in D(A \otimes B)$ , the entropy on each subsystem is the same:

$$H(A) = H(B). \quad (3.5)$$

For isomorphic  $A, A'$ , a maximally entangled state  $\psi \in \mathcal{D}(A \otimes A')$  is a pure state satisfying  $H(A) = \log \dim(A)$ . For a system  $A$  of dimension  $\dim(A)$  and any  $\rho \in D(A \otimes B \otimes C)$ , we have the bounds

$$0 \leq H(A) \leq \log \dim(A), \quad (3.6)$$

$$-H(A) \leq H(A|B) \leq H(A), \quad (3.7)$$

$$0 \leq I(A; B) \leq 2H(A), \quad (3.8)$$

$$0 \leq I(A; B|C) \leq 2H(A). \quad (3.9)$$

The conditional mutual information satisfy a chain rule: for any  $\rho \in D(A \otimes B \otimes C \otimes D)$ ,

$$I(AB; C|D) = I(A; C|D) + I(B; C|AD). \quad (3.10)$$

For product states  $\rho^{A_1 B_1 C_1 A_2 B_2 C_2} = \rho_1^{A_1 B_1 C_1} \otimes \rho_2^{A_2 B_2 C_2}$ , entropy is additive,

$$H(A_1 A_2) = H(A_1) + H(A_2), \quad (3.11)$$

and so there is no conditional mutual information between product system,

$$I(A_1; A_2|B_1 B_2) = 0, \quad (3.12)$$

and conditioning on a product system is useless,

$$I(A_1; B_1|C_1 A_2) = I(A_1; B_1|C_1). \quad (3.13)$$

More generally,

$$I(A_1 A_2; B_1 B_2|C_1 C_2) = I(A_1; B_1|C_1) + I(A_2; B_2|C_2). \quad (3.14)$$

Two important properties of the conditional mutual information are strong subadditivity and the data processing inequality: we consider an equivalent rewriting of strong subadditivity, which states that conditional mutual information is non-negative. For any  $\rho \in \mathcal{D}(A \otimes B \otimes C)$  and  $\mathcal{N} \in \mathcal{C}(B, B')$ , with  $\sigma = \mathcal{N}(\rho)$ ,

$$I(A; B|C)_{\rho} \geq 0, \quad (3.15)$$

$$I(A; B|C)_{\rho} \geq I(A; B'|C)_{\sigma}. \quad (3.16)$$

For classical systems, conditioning is equivalent to taking an average: for any  $\rho^{ABCX} = \sum_x p_X(x) |x\rangle\langle x|^X \otimes \rho_x^{ABC}$ , for a classical system  $X$  and some appropriate  $\rho_x \in \mathcal{D}(A \otimes B \otimes C)$ ,

$$H(A|BX)_\rho = \sum_x p_X(x) H(A|B)_{\rho_x}, \quad (3.17)$$

$$I(A; B|CX)_\rho = \sum_x p_X(x) I(A; B|C)_{\rho_x}. \quad (3.18)$$

### 3.2 Quantum Communication Model

We want to study in full generality the quantum communication complexity of bipartite quantum channels on particular input states. This is the generalization of distributional communication complexity of classical functions to the fully quantum setting, and contains as a special case the distributional quantum communication complexity of classical functions. The model for communication complexity that we consider is the following. For a given bipartite channel  $\mathcal{N} \in \mathcal{C}(A_{in} \otimes B_{in}, A_{out} \otimes B_{out})$  and input state  $\rho \in \mathcal{D}(A_{in} \otimes B_{in})$ , Alice and Bob are given input registers  $A_{in}, B_{in}$  at the outset of the protocol, respectively, and they output registers  $A_{out}, B_{out}$  at the end of the protocol, respectively, which should be in state  $\mathcal{N}(\rho)$ . We generally allow for some small error  $\varepsilon$  in the output, which will be formalized below. In the usual communication complexity setting, the input is be a classical state  $\rho = \sum_{x,y} p_{XY}(x,y) |x\rangle\langle x|^{A_{in}} \otimes |y\rangle\langle y|^{B_{in}}$ , the channel  $\mathcal{N}$  implements a classical functions  $\mathcal{N}(|x\rangle\langle x| \otimes |y\rangle\langle y|) = |f_A(x,y)\rangle\langle f_A(x,y)|^{A_{out}} \otimes |f_B(x,y)\rangle\langle f_B(x,y)|^{B_{out}}$ , and the error parameter is related to the probability of failure  $\sum_{x,y} p_{XY}(x,y) [\Pi(x,y) \neq (f_A(x,y), f_B(x,y))] \leq \frac{\varepsilon}{2}$ , as proved in section 7.1.

A protocol  $\Pi$  for implementing  $\mathcal{N}$  on input  $\rho^{A_{in}B_{in}}$  is defined by a sequence of unitaries  $U_1, \dots, U_{M+1}$  along with a pure state  $\psi \in \mathcal{D}(T_A \otimes T_B)$  shared between Alice and Bob, for arbitrary finite dimensional registers  $T_A, T_B$ . For appropriate finite dimensional memory registers  $A_1, A_3, \dots, A_{M-1}, A'$  held by Alice,  $B_2, B_4, \dots, B_{M-2}, B'$  held by Bob, and communication registers  $C_1, C_2, C_3, \dots, C_M$  exchanged by Alice and Bob, we have (see Figure 1)  $U_1 \in \mathcal{U}(A_{in} \otimes T_A, A_1 \otimes C_1)$ ,  $U_2 \in \mathcal{U}(B_{in} \otimes T_B \otimes C_1, B_2 \otimes C_2)$ ,  $U_3 \in \mathcal{U}(A_1 \otimes C_2, A_3 \otimes C_3)$ ,  $U_4 \in \mathcal{U}(B_2 \otimes C_3, B_4 \otimes C_4)$ ,  $\dots$ ,  $U_M \in \mathcal{U}(B_{M-2} \otimes C_{M-1}, B_{out} \otimes B' \otimes C_M)$ ,  $U_{M+1} \in \mathcal{U}(A_{M-1} \otimes C_M, A_{out} \otimes A')$ . We slightly abuse notation and also write  $\Pi$  to denote the channel implemented by the protocol, i.e.

$$\Pi(\rho) = \text{Tr}_{A'B'}(U_{M+1}U_M \cdots U_2U_1(\rho \otimes \psi)). \quad (3.19)$$

Then we say that a protocol  $\Pi$  for implementing channel  $\mathcal{N}$  on input  $\rho^{A_{in}B_{in}}$ , with purification  $\rho^{A_{in}B_{in}R}$  for a reference system  $R$ , has error  $\varepsilon \in [0, 2]$  if

$$\|\Pi(\rho) - \mathcal{N}(\rho)\|_{A_{out}B_{out}R} \leq \varepsilon. \quad (3.20)$$

We denote the set of all such protocol as  $\mathcal{T}(\mathcal{N}, \rho, \varepsilon)$ . If we want to restrict this set to bounded round protocols with  $M$  messages, we write  $\mathcal{T}^M(\mathcal{N}, \rho, \varepsilon)$ . Note that for simplicity, we only define protocols with an even number of messages; our results also hold without this restriction, though in the special case of one round protocols, we would rather consider bipartite channels with a single output to ensure that the quantum communication complexity is well-defined. The introduction of the reference system  $R$  is essential to ensure that the protocol



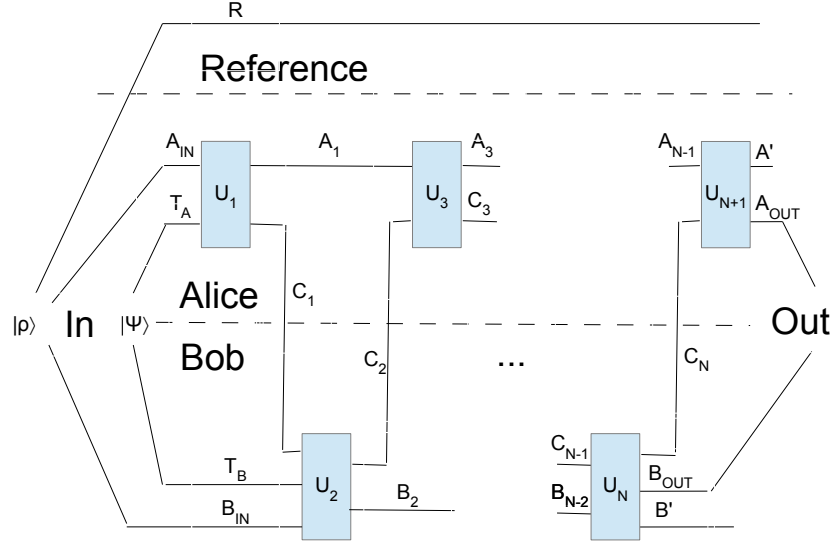


Figure 1: A standard protocol in our quantum communication model

preserves any correlation the input state might have with the outside world as well as the channel it is supposed to implement. As said before, for classical functions on classical input distributions, we prove a lemma in section 7.1 that relates this to the probability of failure of the protocol on such a distribution.

Note that in the standard context of quantum communication complexity, our model would be akin to the model introduced by Cleve and Buhrman [21], with pre-shared entanglement (though the fact that we use quantum communication here instead of classical communication as in the original model could lead to an improvement up to a factor of two of the communication complexity, due to superdense coding [10], but no more, due to the teleportation protocol [7]), rather than to the model introduced by Yao [36], in which parties locally initialize their registers. This is the natural analogue of the framework for classical information complexity in which parties are allowed shared randomness for free, and this seems to be necessary to obtain the operational interpretation of information complexity, classical and quantum, as the amortized communication complexity. Known proofs of the additivity property rely heavily on the availability of shared resources to perform some kind of simulation. This is also true of many other interesting properties of information complexity. Even though additivity and other results might not hold in the Yao model, studying information complexity in this model might still make sense: we would first have to restrict ourselves to protocols in which the pre-shared state  $\psi$  is a pure product state. However, the definition of quantum information complexity would need to be somewhat modified, since the definition we give in section 5 allows for entanglement distribution at no cost, which is consistent with our Cleve-Buhrman like model of communication.

As was said before, our framework is the quantum generalization of the one for distribu-

tional information complexity, and so let us formally define the different quantities that we work with.

**Definition 1** *For a protocol  $\Pi$  as defined above, we define the quantum communication cost of  $\Pi$  as*

$$QCC(\Pi) = \sum_i \log \dim(C_i).$$

Note that we do not require that  $\dim(C_i) = 2^k$  for some  $k \in \mathbb{N}$ , as is usually done. This will not affect our definition on information cost and complexity, nor on amortized communication complexity, but might affect the single-copy quantum communication complexity by at most a factor of two. The corresponding notion of quantum communication complexity of a channel is:

**Definition 2** *For a bipartite channel  $\mathcal{N} \in \mathcal{C}(A_{in} \otimes B_{in}, A_{out} \otimes B_{out})$ , an input state  $\rho \in D(A_{in} \otimes B_{in})$  and an error parameter  $\varepsilon \in [0, 2]$ , we define the  $\varepsilon$ -error quantum communication complexity of  $\mathcal{N}$  on input  $\rho$  as*

$$QCC(\mathcal{N}, \rho, \varepsilon) = \min_{\Pi \in \mathcal{T}(\mathcal{N}, \rho, \varepsilon)} QCC(\Pi).$$

Note that this quantity is discontinuous in its parameters. Also note that no good bound is known on the size of the entangled state that might be required to achieve this minimum. See [32] for a recent discussion on related issues in a different setting. We make the following trivial remark that quantum communication complexity is decreasing in the error parameter, that it vanishes for  $\varepsilon = 2$ , that it is bounded by  $\log \dim(A_{in}) + \log \dim(A_{out})$ , and that it also vanishes for any pure state  $\rho$ . At  $\varepsilon = 2$ , it is because the trace distance is saturated at 2 and so we can consider a protocol that outputs anything without communication, while for pure states it is because there is no correlation with the outside world, so we can consider a protocol that is given, as entanglement for the protocol, the output of the channel acting on the pure state, and outputs it without communication.

**Remark 1** *For any  $\mathcal{N}, \rho, 0 \leq \varepsilon_1 \leq \varepsilon_2 \leq 2$ , the following holds:*

$$\begin{aligned} QCC(\mathcal{N}, \rho, \varepsilon_2) &\leq QCC(\mathcal{N}, \rho, \varepsilon_1), \\ QCC(\mathcal{N}, \rho, 0) &\leq \log \dim(A_{in}) + \log \dim(A_{out}), \\ QCC(\mathcal{N}, \rho, 2) &= 0. \end{aligned}$$

*Also, for any  $\mathcal{N}, \varepsilon \in [0, 2]$ , the following holds for any pure state  $\rho$  :*

$$QCC(\mathcal{N}, \rho, \varepsilon) = 0.$$

We have the following definition for bounded round quantum communication complexity, and similar remarks hold.

**Definition 3** For a bipartite channel  $\mathcal{N} \in \mathcal{C}(A_{in} \otimes B_{in}, A_{out} \otimes B_{out})$ , an input state  $\rho \in D(A_{in} \otimes B_{in})$ , an error parameter  $\varepsilon \in [0, 2]$  and a bound  $M \in \mathbb{N}$  on the number of messages, we define the  $M$ -message,  $\varepsilon$ -error quantum communication complexity of  $\mathcal{N}$  on input  $\rho$  as

$$QCC^M(\mathcal{N}, \rho, \varepsilon) = \min_{\Pi \in \mathcal{T}^M(\mathcal{N}, \rho, \varepsilon)} QCC(\Pi).$$

We are also interested in the amortized quantum communication complexity of channels. A protocol  $\Pi_n$  is said to compute the  $n$ -fold product channel  $\mathcal{N}^{\otimes n}$  on input  $(\rho)^{\otimes n}$  with error  $\varepsilon$  if for all  $i \in [n]$ ,

$$\| \text{Tr}_{-(A_{in}^i B_{in}^i R^i)} \circ \Pi_n(\rho^{\otimes n}) - \mathcal{N}(\rho) \|_{A_{out}^i B_{out}^i R^i} \leq \varepsilon. \quad (3.21)$$

We have implicitly used the fact that it is possible to find a purification of  $\rho^{\otimes n}$  with a decomposition of the purifying register  $R = R_1 \otimes \cdots \otimes R_n$ , and with the  $i$ -th copy of  $\rho$  purified by the reference subregister  $R_i$ . This error criterion corresponds to the one achieved when sequentially simulating  $n$  times channel  $\mathcal{N}$  on input  $\rho$ , each time with error  $\varepsilon$ , and is weaker than demanding to simulate it  $n$  times with overall error  $\varepsilon$ . The reason for this is that asking for overall error  $\varepsilon$  could be a much harder task. Indeed, consider a purified input state that is  $\varepsilon$  away in trace distance to a state which is product with respect to the  $A_{in}B_{in} - R$  bipartite cut. Then, since the trace distance is monotone under noisy channels, the parties can simulate the channel at zero communication cost and achieve error  $\varepsilon$  by taking, as part of the entanglement of their protocol, the  $A_{out}B_{out}$  registers of the channel acting on that product state. Thus the quantum information complexity is also zero. We can then also achieve the task of amortized quantum communication complexity with  $\varepsilon$  error in each input at zero communication. However, using the operational interpretation of the trace distance as the best bias in a distinguishability experiment, the amortized quantum communication task in which we ask for overall error  $\varepsilon$  cannot be achieved at zero communication cost, since having access to many instances of the output state allows for better distinguishability whenever starting with distinguishability greater than zero between the actual input and the product state [6]. Hence, if we want to obtain the intended operational interpretation, we have to settle for such a success parameter. We denote  $\mathcal{T}_n(\mathcal{N}^{\otimes n}, \rho^{\otimes n}, \varepsilon)$  the set of all protocols achieving the above goal of having  $\varepsilon$  error in each output, and can define the  $n$ -fold quantum communication complexity accordingly.

**Definition 4** For a bipartite channel  $\mathcal{N} \in \mathcal{C}(A_{in} \otimes B_{in}, A_{out} \otimes B_{out})$ , an input state  $\rho \in D(A_{in} \otimes B_{in})$  and an error parameter  $\varepsilon \in [0, 2]$ , we define the  $\varepsilon$ -error,  $n$ -fold quantum communication complexity of  $\mathcal{N}$  on input  $\rho$  as

$$QCC_n(\mathcal{N}^{\otimes n}, \rho^{\otimes n}, \varepsilon) = \min_{\Pi_n \in \mathcal{T}_n(\mathcal{N}^{\otimes n}, \rho^{\otimes n}, \varepsilon)} QCC(\Pi_n).$$

**Definition 5** For a bipartite channel  $\mathcal{N} \in \mathcal{C}(A_{in} \otimes B_{in}, A_{out} \otimes B_{out})$ , an input state  $\rho \in D(A_{in} \otimes B_{in})$ , and an error parameter  $\varepsilon \in [0, 2]$ , we define the  $\varepsilon$ -error amortized quantum communication complexity of  $\mathcal{N}$  on input  $\rho$  as

$$AQCC(\mathcal{N}, \rho, \varepsilon) = \limsup_{n \rightarrow \infty} \frac{1}{n} QCC_n(\mathcal{N}^{\otimes n}, \rho^{\otimes n}, \varepsilon).$$

Note that for all  $n$ ,  $QCC_n(\mathcal{N}^{\otimes n}, \rho^{\otimes n}, \varepsilon) \leq nQCC(\mathcal{N}, \rho, \varepsilon)$ , as is made clear by running  $n$  times in parallel a protocol achieving the minimum in the definition of the quantum communication complexity. Hence, the amortized quantum communication complexity is bounded by the quantum communication complexity.

We have corresponding definitions for bounded round complexity.

**Definition 6** For a bipartite channel  $\mathcal{N} \in \mathcal{C}(A_{in} \otimes B_{in}, A_{out} \otimes B_{out})$ , an input state  $\rho \in D(A_{in} \otimes B_{in})$ , an error parameter  $\varepsilon \in [0, 2]$  and a bound  $M \in \mathbb{N}$  on the number of messages, we define the  $M$ -message,  $\varepsilon$ -error,  $n$ -fold quantum communication complexity of  $\mathcal{N}$  on input  $\rho$  as

$$QCC_n^M(\mathcal{N}^{\otimes n}, \rho^{\otimes n}, \varepsilon) = \min_{\Pi_n \in \mathcal{T}_n^M(\mathcal{N}^{\otimes n}, \rho^{\otimes n}, \varepsilon)} QCC(\Pi_n).$$

**Definition 7** For a bipartite channel  $\mathcal{N} \in \mathcal{C}(A_{in} \otimes B_{in}, A_{out} \otimes B_{out})$ , an input state  $\rho \in D(A_{in} \otimes B_{in})$ , an error parameter  $\varepsilon \in [0, 2]$  and a bound  $M \in \mathbb{N}$  on the number of messages, we define the  $M$ -message,  $\varepsilon$ -error amortized quantum communication complexity of  $\mathcal{N}$  on input  $\rho$  as

$$AQCC^M(\mathcal{N}, \rho, \varepsilon) = \limsup_{n \rightarrow \infty} \frac{1}{n} QCC_n^M(\mathcal{N}^{\otimes n}, \rho^{\otimes n}, \varepsilon).$$

## 4 Different Perspective on Classical Information Cost

Before diving into the definition of quantum information cost and the properties of such a definition, we first present a different perspective on the classical information cost that is both natural and more amenable to a quantum generalization. Taking this perspective leads to an alternate proof of its operational interpretation as the amortized (distributional) communication cost. The main difference from the standard definition is not so much in the formal rewriting of this definition, which to some extent was already implicitly used in previous proofs [19, 14] and is simply an application of the chain rule and basic properties of mutual information. It is rather in the interpretation of every message transmission as the simulation of a noisy channel (the generation of the message from the input, previous messages, and randomness) with feedback to the sender and side information at the receiver, a variant of the setting of the classical reverse Shannon theorem studied in the information theory literature [9, 8]. Using a quantum analogue of the reverse Shannon theorem with side information at the receiver [24, 37], this local description of information cost then circumvent usual difficulties in defining a quantum analogue of a transcript, and leads to a generalization of information complexity with the desired properties.

We consider a  $N$ -message classical communication protocol  $\Pi$ , along with a distribution  $\mu$  over the inputs  $(X, Y)$ , and public randomness  $R$ . The protocol is defined by a sequence of conditional random variables  $M_i$  taking value in the sample space  $\{0, 1\}^*$ , with some suitable constraints to enforce that protocols are well-defined. For random variable  $M, I$ , we denote by  $M|I$  the table of conditional transition probabilities  $p_{M|I}(M = m|I = i)$  that gives the probability to obtain output  $M = m$  given input  $I = i$ . Then, on input random variables  $(X, Y)$ ,  $\Pi$  is defined by  $M_1|XR^A, M_2|M_1^B YR^B, M_3|M_2^A M_1^A X R^A, \dots, M_N|M_{N-1}^A \dots M_1^A Y R^A$ , with the

superscripts denoting whose copy of a random variable we are considering. We denote the transcript by  $\Pi(x, y) = r \cdot m_1 \cdot m_2 \cdots m_N$ , and the corresponding random variable by  $\Pi(X, Y)$ . The communication complexity of  $\Pi$  is defined as  $CC(\Pi) = \max |m_1 \cdot m_2 \cdots m_N|$ , in which the maximum for the length is taken over all input pairs  $(x, y) \in (X, Y)$ , over all public randomness  $r \in R$ , and all conditional transcript  $m_1 m_2 \dots m_N \in M_1 M_2 \cdots M_N | (X, Y, R) = (x, y, r)$  (we only consider events with non-zero probability). Sometimes it is also defined by taking the average length instead of the maximum; this does not affect the results here.

The standard definition of the information cost is then as the sum of two conditional mutual informations,

$$IC_\mu(\Pi) = I(\Pi(X, Y); Y|X) + I(\Pi(X, Y); X|Y), \quad (4.1)$$

and the corresponding intuition for this quantity is that it represents the amount of information leaked by the transcript to Alice about Bob's input plus that leaked to Bob about Alice's input. This definition is shown in [19] to lead to an equality between information complexity and the distributional amortized communication complexity. We would like to show such a theorem about an analogous quantum information cost quantity. However, many problems seem to arise when trying to generalize the above quantity to the quantum setting. Before proposing such a definition, we first give an alternate characterization of classical information cost, along with the corresponding operational intuition, which will be more amenable to a quantum generalization. Note that an interesting consequence of our perspective versus those on sampling complexity that have been studied before is that it enables us to use some previously proved tools from information theory, namely (tensor power source) classical reverse Shannon theorems.

We define an alternate information cost for classical communication protocols as

$$IC'_\mu = I(M_1^B; X R^A | Y R^B) + I(M_2^A; Y M_1^B R^B | X M_1^A R^A) \quad (4.2)$$

$$+ I(M_3^B; X M_2^A M_1^A R^A | Y M_2^B M_1^B R^B) + \cdots \quad (4.3)$$

$$+ I(M_N^A; Y M_{N-1}^B \cdots M_1^B R^B | X M_{N-1}^A \cdots M_1^A R^A), \quad (4.4)$$

in which we distinguish between Alice's and Bob's copy of the public randomness  $R$  and messages  $M_i$ . Note that this is easily seen to be equivalent to the standard definition for  $IC_\mu$ , by using the chain rule for mutual information along with the fact that  $M_i^A, M_i^B$  and  $R^A, R^B$  are just copies of one another. However, it is not so much in the formal statement that the rewriting is interesting, but in the operational interpretation. Indeed, the above characterization comes from viewing each conditional message  $M|I$  in the protocol as a noisy channel in which the output  $M$  is sent over a noiseless channel to a receiver who has side information  $S$  about the input  $I$  to the channel, but for which also a copy  $M_F$  of the output is given as feedback to the sender. The problem of simulating the sending of the output of a noisy channel with feedback has been studied in the literature under the name of classical reverse Shannon theorem [9, 8], and when there is side information  $S$  at the receiver,  $I(M; I|S)$  characterizes the amount of information that needs to be sent over the noiseless channel from sender to receiver. It is shown in [31] that asymptotically, this task can be accomplished at a (unidirectional) classical communication rate of  $I(M; I|S)$  when sufficient shared randomness is present. In [19], a correlated sampling protocol is

used to perform a similar task in a one-shot setting, but such that the same communication efficiency is achieved on average, to first order. A caveat is that their protocol to do so is interactive, while the one in [31] is not. This result yields a simulation protocol for amortized communication that asymptotically achieves communication at the information cost of the protocol, while keeping the same round complexity, and error parameter arbitrarily close to the original one. Another nice property of reverse Shannon theorems is that they also give bounds on the amount of extra shared randomness required in the asymptotic limit for channel simulation. We do not give the details of the proof here, it follows along the same line as the one for the quantum case. We also do not discuss optimality here (see the quantum case, or [19, 14] for such discussions).

## 5 Quantum Information Cost and Complexity

Finally, we are ready to define quantum information cost and complexity ! As we already said, the notion of information cost of a protocol does not seem to easily extend to the quantum setting, mainly due to the fact that there is no direct analogue for a transcript in the quantum setting. Also, the reversibility of quantum computation allows for protocols in which nothing remains at the end of the distributed computation except for the initial inputs and the output of the function evaluated on these inputs (up to some small error for approximate protocols). These issues brought Braverman [14] to wonder what was the right quantum analogue of information cost, and whether there always existed protocols for computing binary functions that had quantum information cost bounded by a constant. Some attempts at trying to define a quantum analogue of information cost have appeared before [27, 26], and have proven useful for tackling particular problems. However, none of these seems to define the right notion in a context of amortized communication complexity. In particular there is an implicit dependence on the round complexity for these notions, and they only provide a lower bound on the communication cost once divided by the number of rounds. Defining such a notion would hopefully lead to an interesting tool, in particular to obtain lower bounds and to tackle direct sum questions in quantum communication complexity. The main goal of our work is to present such a notion in a strong sense: we define a notion of quantum information complexity which is exactly equal to the amortized communication complexity.

From the alternate definition of the information cost in the preceding section, we can more easily extend it to a notion of quantum information cost for quantum protocols. A thing that might still cause problem is that we cannot keep a copy of a channel input and output at the sender. These issues have already been discussed in particular when discussing connections between the fully quantum Slepian-Wolf theorem [2] and the fully quantum reverse Shannon theorem [8, 11], and when discussing the fully quantum generalization of channel simulation with side information at the receiver [31, 24, 37]. The correct quantum analogue of this is that what stays at the sender is the coherent feedback of the environment output of the noisy channel's isometric extension, and what is to be transmitted at the receiver is the usual output of the channel. In our situation, there is also another system in play, the side information already in the possession of the receiver before the transmission. The correct problem to consider in this case is then quantum state redistribution [31, 24, 37]. In

quantum state redistribution, there are 4 systems of interest. At the outset of the protocol, the  $A, C$  systems are in the possession of Alice, and would be for us the coherent feedback of the noisy channel and the output to be transmitted, respectively, while Bob holds the side information  $B$ , and the  $ABC$  joint system is purified by a reference register  $R$  that no party has access to. Thus, the only system changing hands is the  $C$  subsystem that is to be transmitted from Alice to Bob. It is proved in [24, 37] that this can be accomplished, in the limit of asymptotically many copies of this task, at a communication cost of  $\frac{1}{2}I(R; C|B)$  qubits per copy, along with an entanglement cost of  $\frac{1}{2}I(C; A) - \frac{1}{2}I(C; B)$  ebits per copy (with entanglement generated instead of consumed if this is negative). We state a precise formulation of this theorem.

**Theorem 1** (State redistribution [24, 37]) *For any  $\varepsilon, \delta > 0$ , any state  $\rho^{ABC}$  and any purification  $\rho^{ABCR}$ , any quantum communication rate  $Q > \frac{1}{2}I(C; R|B)$  and entanglement consumption (or generation if negative) rate  $E$  satisfying  $Q + E > H(C|B)$ , there is a large enough  $n_0$  such that for all  $n \geq n_0$ , there exist an encoder  $E \in C(A^{\otimes n} \otimes C^{\otimes n} \otimes T_A^{\text{in}}, A^{\otimes n} \otimes \hat{C} \otimes T_A^{\text{out}})$  and a decoder  $D \in C(B^{\otimes n} \otimes \hat{C} \otimes T_B^{\text{in}}, B^{\otimes n} \otimes C^{\otimes n} \otimes T_B^{\text{out}})$  such that  $\dim(T_A^{\text{in}}) = \dim(T_B^{\text{in}}) = 2^{\lceil \max(E, \delta)n \rceil}$ ,  $\dim(T_A^{\text{out}}) = \dim(T_B^{\text{out}}) = 2^{-\lceil \min(0, E)n \rceil}$ ,  $\dim(\hat{C}) = 2^{\lceil Qn \rceil}$ ,  $\psi_{\text{in}}^{T_A^{\text{in}} T_B^{\text{in}}}, \psi_{\text{out}}^{T_A^{\text{out}} T_B^{\text{out}}}$  are maximally entangled states in  $T_A^{\text{in}} \otimes T_B^{\text{in}}, T_A^{\text{out}} \otimes T_B^{\text{out}}$ , respectively, and*

$$\| \text{Tr}_{T_A^{\text{out}} T_B^{\text{out}}} \circ D \circ E(\rho^{\otimes n} \otimes \psi_{\text{in}}) - \rho^{\otimes n} \|_{A^{\otimes n} B^{\otimes n} C^{\otimes n} R^{\otimes n}} \leq \varepsilon, \quad (5.1)$$

$$\| \text{Tr}_{T_A^{\text{out}} T_B^{\text{out}}} \circ D \circ E(\rho^{\otimes n} \otimes \psi_{\text{in}}) - \psi_{\text{out}} \|_{T_A^{\text{out}} T_B^{\text{out}}} \leq \varepsilon. \quad (5.2)$$

Now, in analogy with our rewriting of the classical information cost, we define the quantum information cost of a protocol, for a protocol  $\Pi$  as defined in section 3.2, in the following way.

**Definition 8** *For a protocol  $\Pi$  and an input state  $\rho$ , we define the quantum information cost of  $\Pi$  on input  $\rho$  as*

$$QIC(\Pi, \rho) = \sum_{i>0, \text{odd}} \frac{1}{2} I(C_i; R|B_{i-1}) + \sum_{i>0, \text{even}} \frac{1}{2} I(C_i; R|A_{i-1}),$$

in which we have labelled  $B_0 = B_{\text{in}} \otimes T_B$ .

Note that even for protocols with non-zero communication, the quantum information cost on pure state input is zero, since the purifying  $R$  register is trivial in such a case. The corresponding notion of quantum information complexity of a channel is then:

**Definition 9** *For a bipartite channel  $\mathcal{N} \in \mathcal{C}(A_{\text{in}} \otimes B_{\text{in}}, A_{\text{out}} \otimes B_{\text{out}})$ , an input state  $\rho \in \mathcal{D}(A_{\text{in}} \otimes B_{\text{in}})$  and an error parameter  $\varepsilon \in [0, 2]$ , we define the  $\varepsilon$ -error quantum information complexity of  $\mathcal{N}$  on input  $\rho$  as*

$$QIC(\mathcal{N}, \rho, \varepsilon) = \inf_{\Pi \in \mathcal{T}(\mathcal{N}, \rho, \varepsilon)} QIC(\Pi, \rho).$$

We have the following operational interpretation for quantum information complexity as the amortized quantum communication complexity.

**Theorem 2** For a bipartite channel  $\mathcal{N} \in \mathcal{C}(A_{in} \otimes B_{in}, A_{out} \otimes B_{out})$ , an input state  $\rho \in \mathcal{D}(A_{in} \otimes B_{in})$  and an error parameter  $\varepsilon \in (0, 2]$ ,

$$QIC(\mathcal{N}, \rho, \varepsilon) = AQCC(\mathcal{N}, \rho, \varepsilon).$$

The proof of the theorem is given in section 6.5. We can also obtain bounded round variants.

**Definition 10** For a bipartite channel  $\mathcal{N} \in \mathcal{C}(A_{in} \otimes B_{in}, A_{out} \otimes B_{out})$ , an input state  $\rho \in \mathcal{D}(A_{in} \otimes B_{in})$ , an error parameter  $\varepsilon \in [0, 2]$  and a bound  $M \in \mathbb{N}$  on the number of messages, we define the  $M$ -message,  $\varepsilon$ -error quantum information complexity of  $\mathcal{N}$  on input  $\rho$  as

$$QIC^M(\mathcal{N}, \rho, \varepsilon) = \inf_{\Pi \in \mathcal{T}^M(\mathcal{N}, \rho, \varepsilon)} QIC(\Pi, \rho).$$

**Theorem 3** For a bipartite channel  $\mathcal{N} \in \mathcal{C}(A_{in} \otimes B_{in}, A_{out} \otimes B_{out})$ , an input state  $\rho \in \mathcal{D}(A_{in} \otimes B_{in})$ , an error parameter  $\varepsilon \in (0, 2]$  and a bound  $M \in \mathbb{N}$  on the number of messages,

$$QIC^M(\mathcal{N}, \rho, \varepsilon) = AQCC^M(\mathcal{N}, \rho, \varepsilon).$$

## 6 Properties of the Definition

### 6.1 Quantum information lower bounds communication

In this section, we make the important remark that in any protocol, the quantum information cost is non-negative and, more importantly, is a lower bound on the quantum communication cost. This holds when considering the quantum information cost with respect to any input state. This follows from the fact for any quantum state,  $0 \leq \frac{1}{2}I(C; R|B) \leq \log \dim(C)$ . Applying this to all terms in the quantum information cost versus all terms in the quantum communication cost, we get the result. A similar results holds for quantum information complexity versus quantum communication complexity, by taking infimum on both sides.

**Lemma 1** For any protocol  $\Pi$  and input state  $\rho$ , the following holds

$$0 \leq QIC(\Pi, \rho) \leq QCC(\Pi).$$

**Corollary 1** For any channel  $\mathcal{N}$ , any input state  $\rho$ , any error parameter  $\varepsilon \in [0, 2]$  and any bound  $M \in \mathbb{N}$  on the number of messages, the following holds

$$\begin{aligned} QIC(\mathcal{N}, \rho, \varepsilon) &\leq QCC(\mathcal{N}, \rho, \varepsilon), \\ QIC^M(\mathcal{N}, \rho, \varepsilon) &\leq QCC^M(\mathcal{N}, \rho, \varepsilon). \end{aligned}$$



## 6.2 Quantum information upper bounds amortized communication

We now prove some kind of converse result to the one in the previous section: the quantum information cost is an upper bound on the amortized quantum communication cost.

**Lemma 2** *For any  $M$ -message protocol  $\Pi$ , any input state  $\rho$  and any  $\varepsilon \in (0, 2], \delta > 0$ , there exists a large enough  $n_0$  such that for any  $n \geq n_0$ , there exists a protocol  $\Pi_n \in \mathcal{T}^M(\Pi^{\otimes n}, \rho^{\otimes n}, \varepsilon)$  satisfying*

$$\frac{1}{n} QCC(\Pi_n) \leq QIC(\Pi, \rho) + \delta.$$

**Proof.** Given any  $M$ -message protocol  $\Pi$  and any state  $\rho^{A_{in} B_{in} R}$ , let

$$\rho_1^{A_1 C_1 B_0 R} = U_1(\rho \otimes \psi), \rho_2^{A_1 C_2 B_2 R} = U_2(\rho_1), \dots, \rho_M^{A_{M-1} C_M B_M R} = U_M(\rho_{M-1})$$

in which we label  $B_0 = B_{in} \otimes T_B, B_M = B_{out} \otimes B'$ . Then, for any  $\varepsilon, \delta > 0$ , take  $Q_i = \frac{1}{2} I(C_i; R | B_{i-1}) + \frac{\delta}{2M}$  and  $F_i = \frac{1}{2} \max(0, I(C_i; A_i) - I(C_i; B_{i-1})) + \frac{\delta}{2M}$  for  $i$  odd (we do not worry here about reusing the possibly generated entanglement, and simply discard it in the encoding and decoding maps to be defined below),  $Q_i = \frac{1}{2} I(C_i; R | A_{i-1}) + \frac{\delta}{2M}$  and  $F_i = \frac{1}{2} \max(0, I(C_i; B_i) - I(C_i; A_{i-1})) + \frac{\delta}{2M}$  for  $i$  even, and for each  $i$  let  $n_0^i$  be the corresponding  $n_0$  for error  $\frac{\varepsilon}{M}$  in Theorem 1, and take  $n_0 = \max\{n_0^i\}$ . Then for any  $n \geq \max(n_0, \frac{2M}{\delta})$ , we have encoding and decoding maps  $E_i, D_i$ , along with corresponding entanglement  $\psi_i \in D(T_A^i \otimes T_B^i)$  and communication register  $\hat{C}^i$  of size  $\dim \hat{C}^i = 2^{\lceil Q_i n \rceil}$ , with each satisfying

$$\|D_i \circ E_i(\rho_i^{\otimes n} \otimes \psi_i) - \rho_i^{\otimes n}\|_{A_i^{\otimes n} C_i^{\otimes n} B_{i-1}^{\otimes n} R^{\otimes n}} \leq \frac{\varepsilon}{M} \quad (6.1)$$

for odd  $i$ , or

$$\|D_i \circ E_i(\rho_i^{\otimes n} \otimes \psi_i) - \rho_i^{\otimes n}\|_{A_{i-1}^{\otimes n} C_i^{\otimes n} B_i^{\otimes n} R^{\otimes n}} \leq \frac{\varepsilon}{M} \quad (6.2)$$

for even  $i$ . Let  $\hat{E}_i, \hat{D}_i$  be unitary extensions of  $E_i, D_i$ , respectively, requiring ancillary states  $\sigma_i^E \in \mathcal{D}(E_i^{in}), \sigma_i^D \in \mathcal{D}(D_i^{in})$ . We define the following protocol  $\Pi_n$  starting from the protocol  $\Pi$ .

---

Protocol  $\Pi_n$  on input  $\sigma$ :

- Take entangled state  $\hat{\psi} = \psi^{\otimes n} \otimes \psi_1 \otimes \sigma_1^E \otimes \sigma_1^D \otimes \dots \otimes \psi_M \otimes \sigma_M^E \otimes \sigma_M^D$ .
  - Take unitaries  $\hat{U}_1 = \hat{E}_1 \circ U_1^{\otimes n}, \hat{U}_2 = \hat{E}_2 \circ U_2^{\otimes n} \circ \hat{D}_1, \dots, \hat{U}_M = \hat{E}_M \circ U_M^{\otimes n} \circ \hat{D}_{M-1}, \hat{U}_{M+1} = U_{M+1}^{\otimes n} \circ \hat{D}_M$
  - Take as output the  $A_{out}^{\otimes n}, B_{out}^{\otimes n}$  registers.
-

Note that the communication cost of  $\Pi_n$  satisfies

$$\begin{aligned}
QCC(\Pi_n) &= \sum_i \log \dim(\hat{C}^i) \\
&= \sum_i \lceil Q_i n \rceil \\
&\leq n \left( \sum_{i>0, \text{odd}} \frac{1}{2} I(C_i; R|B_{i-1}) + \sum_{i>0, \text{even}} \frac{1}{2} I(C_i; R|A_{i-1}) + \frac{M\delta}{2M} + \frac{M}{n} \right) \\
&\leq n(QIC(\Pi, \rho) + \delta).
\end{aligned}$$

This is also a  $M$ -message protocol, so is left to bound the error on input  $\sigma = \rho^{\otimes n}$  to make sure that  $\Pi_n \in \mathcal{T}(\Pi^{\otimes n}, \rho^{\otimes n}, \varepsilon)$ . We have

$$\begin{aligned}
\|\Pi_n(\rho^{\otimes n}) - \Pi^{\otimes n}(\rho^{\otimes n})\| &= \|\text{Tr}_{\neg A_{out}^{\otimes n} B_{out}^{\otimes n}} U_{M+1}^{\otimes n} \hat{D}_M \hat{E}_M U_M^{\otimes n} \hat{D}_{M-1} \cdots \hat{E}_1 U_1^{\otimes n} (\rho^{\otimes n} \otimes \hat{\psi}) \\
&\quad - \text{Tr}_{\neg A_{out}^{\otimes n} B_{out}^{\otimes n}} U_{M+1}^{\otimes n} U_M^{\otimes n} \cdots U_1^{\otimes n} (\rho^{\otimes n} \otimes \psi^{\otimes n})\| \\
&= \|\text{Tr}_{\neg A_{out}^{\otimes n} B_{out}^{\otimes n}} U_{M+1}^{\otimes n} D_M E_M U_M^{\otimes n} D_{M-1} \cdots E_1 U_1^{\otimes n} (\rho^{\otimes n} \otimes \psi^{\otimes n} \otimes \psi_1 \otimes \cdots \otimes \psi_M) \\
&\quad - \text{Tr}_{\neg A_{out}^{\otimes n} B_{out}^{\otimes n}} U_{M+1}^{\otimes n} U_M^{\otimes n} \cdots U_1^{\otimes n} (\rho^{\otimes n} \otimes \psi^{\otimes n})\| \\
&\leq \|\text{Tr}_{(A')^{\otimes n} (B')^{\otimes n}} U_{M+1}^{\otimes n} D_M \cdots E_2 U_2^{\otimes n} D_1 E_1 (\rho_1^{\otimes n} \otimes \psi_1 \otimes \cdots \otimes \psi_M) \\
&\quad - \text{Tr}_{(A')^{\otimes n} (B')^{\otimes n}} U_{M+1}^{\otimes n} D_M \cdots E_2 U_2^{\otimes n} (\rho_1^{\otimes n} \otimes \psi_2 \otimes \cdots \otimes \psi_M)\| \\
&+ \|\text{Tr}_{(A')^{\otimes n} (B')^{\otimes n}} U_{M+1}^{\otimes n} D_M E_M U_M^{\otimes n} D_{M-1} \cdots U_3^{\otimes n} D_2 E_2 (\rho_2^{\otimes n} \otimes \psi_2 \otimes \cdots \otimes \psi_M) \\
&\quad - \text{Tr}_{(A')^{\otimes n} (B')^{\otimes n}} U_{M+1}^{\otimes n} D_M E_M U_M^{\otimes n} D_{M-1} \cdots E_3 U_3^{\otimes n} (\rho_2^{\otimes n} \otimes \psi_3 \otimes \cdots \otimes \psi_M)\| \\
&\quad + \cdots \\
&+ \|\text{Tr}_{(A')^{\otimes n} (B')^{\otimes n}} U_{M+1}^{\otimes n} D_M E_M U_M^{\otimes n} D_{M-1} E_{M-1} (\rho_{M-1}^{\otimes n} \otimes \psi_{M-1} \otimes \psi_M) \\
&\quad - \text{Tr}_{(A')^{\otimes n} (B')^{\otimes n}} U_{M+1}^{\otimes n} D_M E_M U_M^{\otimes n} (\rho_{M-1}^{\otimes n} \otimes \psi_M)\| \\
&+ \|\text{Tr}_{(A')^{\otimes n} (B')^{\otimes n}} U_{M+1}^{\otimes n} D_M E_M (\rho_M^{\otimes n} \otimes \psi_M) \\
&\quad - \text{Tr}_{(A')^{\otimes n} (B')^{\otimes n}} U_{M+1}^{\otimes n} (\rho_M^{\otimes n})\| \\
&\leq \|D_1 E_1 (\rho_1^{\otimes n} \otimes \psi_1 \otimes \psi_2 \otimes \cdots \otimes \psi_M) - (\rho_1^{\otimes n} \otimes \psi_2 \otimes \cdots \otimes \psi_M)\| \\
&\quad + \|D_2 E_2 (\rho_2^{\otimes n} \otimes \psi_2 \otimes \psi_3 \otimes \cdots \otimes \psi_M) - (\rho_2^{\otimes n} \otimes \psi_3 \otimes \cdots \otimes \psi_M)\| \\
&\quad + \cdots \\
&\quad + \|D_{M-1} E_{M-1} (\rho_{M-1}^{\otimes n} \otimes \psi_{M-1} \otimes \psi_M) - (\rho_{M-1}^{\otimes n} \otimes \psi_M)\| \\
&\quad + \|D_M E_M (\rho_M^{\otimes n} \otimes \psi_M) - (\rho_M^{\otimes n})\| \\
&\leq M \frac{\varepsilon}{M} \\
&= \varepsilon.
\end{aligned}$$

The first equality is by definition, the second one by tracing the registers  $E_i^{out}, D_i^{out}$  from the unitary extensions to the encoders and decoders in the first term, the first inequality is by the triangle inequality and by definition of the  $\rho_i$ 's, the second inequality is due to the monotonicity of trace distance under noisy channels, and the next is by (6.1) and (6.2), along with the fact that appending uncorrelated systems does not change the trace distance.

We also note that on top of the entanglement  $\psi$  used by each compressed copy of the protocol, the asymptotic entanglement consumption (or generation) rate is bounded by the initial quantum communication cost, which follows from  $-\log \dim(C) \leq \frac{1}{2}(I(C; A) - I(C; B)) \leq \log \dim(C)$ .

■

### 6.3 Additivity

We now show that quantum information complexity satisfy an additivity property. This is used in the converse part of the proof of Theorem 2. Let us set some notation first. We say that a triple  $(\mathcal{N}, \rho, \varepsilon)$  is a quantum task, corresponding to the simulation of channel  $\mathcal{N} \in C(A_{in} \otimes B_{in}, A_{out} \otimes B_{out})$  on input  $\rho \in \mathcal{D}(A_{in} \otimes B_{in})$  with error  $\varepsilon \in [0, 2]$ . We define a product quantum task recursively, and with the following notation: a quantum task is a product quantum task, and if  $T_1 = (\mathcal{N}_1, \rho_1, \varepsilon_1) \otimes \cdots \otimes (\mathcal{N}_i, \rho_i, \varepsilon_i)$ ,  $T_2 = (\mathcal{N}_{i+1}, \rho_{i+1}, \varepsilon_{i+1}) \otimes \cdots \otimes (\mathcal{N}_n, \rho_n, \varepsilon_n)$  are two product quantum tasks, then  $T_1 \otimes T_2 = \bigotimes_{i \in [n]} (\mathcal{N}_i, \rho_i, \varepsilon_i)$  is also a product quantum task. We say that a protocol  $\Pi_n$ , with input space  $A_{in}^1 \otimes B_{in}^1 \otimes \cdots \otimes A_{in}^n \otimes B_{in}^n$  and output space  $A_{out}^1 \otimes B_{out}^1 \otimes \cdots \otimes A_{out}^n \otimes B_{out}^n$ , succeeds at the product quantum task  $\bigotimes_i (\mathcal{N}_i, \rho_i, \varepsilon_i)$  if it succeeds, for each  $i$ , at simulating channel  $\mathcal{N}_i$  on input  $\rho_i$  with error  $\varepsilon_i$ , and denote by  $\mathcal{T}_{\otimes}(\bigotimes_i (\mathcal{N}_i, \rho_i, \varepsilon_i))$  the set of all protocols achieving this. Once again, if we restrict this set to  $M$ -message protocols, we write  $\mathcal{T}_{\otimes}^M(\bigotimes_i (\mathcal{N}_i, \rho_i, \varepsilon_i))$ . We then define the quantum information complexity of the product quantum task  $\bigotimes_i (\mathcal{N}_i, \rho_i, \varepsilon_i)$  as

$$QIC_{\otimes}(\bigotimes_i (\mathcal{N}_i, \rho_i, \varepsilon_i)) = \inf_{\Pi_n \in \mathcal{T}_{\otimes}(\bigotimes_i (\mathcal{N}_i, \rho_i, \varepsilon_i))} QIC(\Pi_n, \rho_1 \otimes \cdots \otimes \rho_n). \quad (6.3)$$

For the bounded round variant, we have

$$QIC_{\otimes}^M(\bigotimes_i (\mathcal{N}_i, \rho_i, \varepsilon_i)) = \inf_{\Pi_n \in \mathcal{T}_{\otimes}^M(\bigotimes_i (\mathcal{N}_i, \rho_i, \varepsilon_i))} QIC(\Pi_n, \rho_1 \otimes \cdots \otimes \rho_n). \quad (6.4)$$

We first prove the following two technical lemmata that will lead to the additivity result.

**Lemma 3** *For any two protocols  $\Pi^1, \Pi^2$  with  $M_1, M_2$  messages, respectively, there exists a  $M$ -message protocol  $\Pi_2$ , satisfying  $\Pi_2 = \Pi^1 \otimes \Pi^2$ ,  $M = \max(M_1, M_2)$ , such that the following holds for any corresponding input states  $\rho^1, \rho^2$ :*

$$QIC(\Pi_2, \rho^1 \otimes \rho^2) = QIC(\Pi^1, \rho^1) + QIC(\Pi^2, \rho^2).$$

**Proof.** Given protocols  $\Pi^1$  and  $\Pi^2$ , we assume without loss of generality that  $M_1 \geq M_2$ , and we define the protocol  $\Pi_2$  in the following way.

---

Protocol  $\Pi_2$  on input  $\sigma$ :

- Run protocols  $\Pi^1, \Pi^2$  in parallel for  $M_2$  messages, on corresponding input registers  $A_{in}^1, B_{in}^1, A_{in}^2, B_{in}^2$  until  $\Pi^2$  has finished.
  - Finish running protocol  $\Pi^1$ .
  - Take as output the output registers  $A_{out}^1, B_{out}^1, A_{out}^2, B_{out}^2$  of both  $\Pi^1$  and  $\Pi^2$ .
-

It is clear that the channel that  $\Pi_2$  implements is  $\Pi_2 = \Pi^1 \otimes \Pi^2$ , and the number of messages satisfies  $M = \max(M_1, M_2)$ , so is left to analyse its quantum information cost on input  $\sigma = \rho_1 \otimes \rho_2$ . The first thing to notice is that we can find a purification of  $\rho_1 \otimes \rho_2$  that is also in product form, i.e. there exist a purification with the purifying system  $R = R^1 \otimes R^2$  and such that  $(\rho_1 \otimes \rho_2)^{A_{in}^1 B_{in}^1 A_{in}^2 B_{in}^2 R} = \rho_1^{A_{in}^1 B_{in}^1 R^1} \otimes \rho_2^{A_{in}^2 B_{in}^2 R^2}$ . Also note that throughout the protocol, due to the structure of  $\Pi_2$  and the fact that the input  $\rho_1 \otimes \rho_2$  is in product form, any registers corresponding to  $\Pi^1$  stays in product form with any register corresponding to  $\Pi^2$ . We label, for  $i \in \{1, 2\}$ ,  $A_0^i = A_{in}^i \otimes T_A^i$ ,  $B_0^i = B_{in}^i \otimes T_B^i$ ,  $A_{M_i}^i = A_{out}^i \otimes (A')^i$ ,  $B_{M_i}^i = B_{out}^i \otimes (B')^i$ . Then

$$\begin{aligned} QIC(\Pi_2, \rho_1 \otimes \rho_2) &= I(C_1^1 C_1^2; R^1 R^2 | B_0^1 B_0^2) + I(C_2^1 C_2^2; R^1 R^2 | A_1^1 A_1^2) \\ &\quad + \dots + I(C_{M_2}^1 C_{M_2}^2; R^1 R^2 | A_{M_2-1}^1 A_{M_2-1}^2) \\ &\quad + I(C_{M_2+1}^1; R^1 R^2 | B_{M_2}^1 B_{M_2}^2) + \dots + I(C_{M_1}^1; R^1 R^2 | A_{M_1-1}^1 A_{M_1-1}^2) \\ &= I(C_1^1; R^1 | B_0^1) + I(C_2^1; R^1 | A_1^1) + \dots + I(C_{M_1}^1; R^1 | A_{M_1-1}^1) \\ &\quad + I(C_1^2; R^2 | B_0^2) + I(C_2^2; R^2 | A_1^2) + \dots \\ &= QIC(\Pi^1, \rho_1) + QIC(\Pi^2, \rho_2). \end{aligned}$$

The first equality is by definition of quantum information cost of  $\Pi_2$ , and due to its parallel structure, the second equality is because registers of  $\Pi^1, \Pi^2$  are in product form, and then the last equality follows from definition and the structure of  $\Pi_2$ . ■

**Lemma 4** For any  $M$ -message protocol  $\Pi_2$  and any input states  $\rho^1 \in \mathcal{D}(A_{in}^1 \otimes B_{in}^1)$ ,  $\rho^2 \in \mathcal{D}(A_{in}^2 \otimes B_{in}^2)$ , there exist  $M$ -message protocols  $\Pi^1, \Pi^2$  satisfying  $\Pi^1(\cdot) = \text{Tr}_{A_{out}^2 B_{out}^2} \circ \Pi_2(\cdot \otimes \rho^2)$ ,  $\Pi^2(\cdot) = \text{Tr}_{A_{out}^1 B_{out}^1} \circ \Pi_2(\rho^1 \otimes \cdot)$ , and the following holds:

$$QIC(\Pi^1, \rho^1) + QIC(\Pi^2, \rho^2) = QIC(\Pi_2, \rho^1 \otimes \rho^2).$$

**Proof.** Given  $\Pi_2$ , we define the protocols  $\Pi^1, \Pi^2$  in the following way.

---

Protocol  $\Pi^1$  on input  $\sigma^1$ :

- Let  $(\rho^2)^{A_{in}^2 B_{in}^2 R^2}$  be a purification of  $\rho^2$ , and  $\psi^{T_A T_B}$  be the entangled state used in the  $\Pi_2$  protocol. The entangled state for the protocol will be  $\rho^2 \otimes \psi$ , with the  $A_{in}^2, R^2, T_A$  registers given to Alice, and the  $B_{in}^2, T_B$  registers given to Bob.
- Using the  $\rho^2$  state given as pre-shared entanglement to simulate the other input, run protocol  $\Pi_2$  on input  $\sigma_1 \otimes \rho_2$ .
- Take as output the  $A_{out}^1 B_{out}^1$  output registers.

---

Protocol  $\Pi^2$  on input  $\sigma^2$ :

- Let  $(\rho^1)^{A_{in}^1 B_{in}^1 R^1}$  be a purification of  $\rho^1$ , and  $\psi^{T_A T_B}$  be the entangled state used in the  $\Pi_2$  protocol. The entangled state for the protocol will be  $\rho^1 \otimes \psi$ , with the  $A_{in}^1, T_A$  registers given to Alice, and the  $B_{in}^1, R^1, T_B$  registers given to Bob.
  - Using the  $\rho^1$  state given as pre-shared entanglement to simulate the other input, run protocol  $\Pi_2$  on input  $\rho^1 \otimes \sigma^2$ .
  - Take as output the  $A_{out}^2 B_{out}^2$  output registers.
-

It is clear that for any  $\sigma^1 \in \mathcal{D}(A_{in}^1 \otimes B_{in}^1), \sigma^2 \in \mathcal{D}(A_{in}^2 \otimes B_{in}^2)$ ,  $\Pi^1, \Pi^2$  implement  $\Pi^1(\sigma^1) = \text{Tr}_{A_{out}^2 B_{out}^2} \circ \Pi_2(\sigma^1 \otimes \rho^2), \Pi^2(\sigma^2) = \text{Tr}_{A_{out}^1 B_{out}^1} \circ \Pi_2(\rho^1 \otimes \sigma^2)$ , respectively. Also,  $\Pi^1, \Pi^2$  are  $M$ -message protocols, so is left to analyse their quantum information costs on input  $\rho^1, \rho^2$ , respectively. We reuse the notation from the previous lemma. By definition and the structure of the protocols,

$$\begin{aligned} QIC(\Pi^1, \rho^1) &= I(C_1; R^1|B_0) + I(C_2; R^1|A_1 R^2) + \dots, \\ QIC(\Pi^2, \rho^2) &= I(C_1; R^2|B_0 R^1) + I(C_2; R^2|A_1) + \dots, \end{aligned}$$

and we get by rearranging terms

$$\begin{aligned} QIC(\Pi^1, \rho^1) + QIC(\Pi^2, \rho^2) &= I(C_1; R^1|B_0) + I(C_1; R^2|B_0 R^1) \\ &\quad + I(C_2; R^1|A_1 R^2) + I(C_2; R^2|A_1) + \dots \\ &= I(C_1; R^1 R^2|B_0) + I(C_2; R^1 R^2|A_1) + \dots \\ &= QIC(\Pi_2, \rho_1 \otimes \rho_2) \end{aligned}$$

where we have used the structure of the protocols along with the chain rule for mutual information on pairs of terms for the second equality, and the last equality follow from definition and the structure of the protocols.

■

We then get as a corollary the following additivity result:

**Corollary 2** *For any two product quantum tasks  $T_1, T_2$  and any bound  $M \in \mathbb{N}$  on the number of messages,*

$$\begin{aligned} QIC_{\otimes}(T_1 \otimes T_2) &= QIC_{\otimes}(T_1) + QIC_{\otimes}(T_2), \\ QIC_{\otimes}^M(T_1 \otimes T_2) &= QIC_{\otimes}^M(T_1) + QIC_{\otimes}^M(T_2). \end{aligned}$$

**Proof.** We consider the two product tasks  $T_1 = \bigotimes_i (\mathcal{N}_i, \rho_i, \varepsilon_i), T_2 = \bigotimes_j (\mathcal{M}_j, \sigma_j, \delta_j)$ . We first prove the  $\leq$  direction. Let  $\Pi^1$  and  $\Pi^2$  be protocols succeeding at the corresponding tasks  $T_1, T_2$ , and achieving, for an arbitrary small  $\varepsilon' > 0$ ,  $QIC(\Pi^1, \rho_1 \otimes \dots \otimes \rho_n) \leq QIC_{\otimes}(T_1) + \varepsilon', QIC(\Pi^2, \sigma_1 \otimes \dots \otimes \sigma_m) \leq QIC_{\otimes}(T_2) + \varepsilon'$ , respectively. Taking the corresponding protocol  $\Pi_2$  from Lemma 3, it clearly succeeds at the product task  $T_1 \otimes T_2$ , and we get

$$\begin{aligned} QIC_{\otimes}(T_1 \otimes T_2) &\leq QIC(\Pi_2, \rho_1 \otimes \dots \otimes \rho_n \otimes \sigma_1 \otimes \dots \otimes \sigma_m) \\ &= QIC(\Pi^1, \rho_1 \otimes \dots \otimes \rho_n) + QIC(\Pi^2, \sigma_1 \otimes \dots \otimes \sigma_m) \\ &\leq QIC_{\otimes}(T_1) + QIC_{\otimes}(T_2) + 2\varepsilon'. \end{aligned}$$

Now for the  $\geq$  direction, let  $\Pi_2$  be a protocol succeeding at the product task and achieving  $QIC(\Pi_2, \rho_1 \otimes \dots \otimes \rho_n \otimes \sigma_1 \otimes \dots \otimes \sigma_m) \leq QIC_{\otimes}(T_1 \otimes T_2) + \varepsilon'$  for an arbitrary small  $\varepsilon' > 0$ . Taking the corresponding protocols  $\Pi^1, \Pi^2$  from Lemma 4 for tasks  $T_1, T_2$ , they clearly succeed at their respective task, and we get

$$\begin{aligned} QIC_{\otimes}(T_1) + QIC_{\otimes}(T_2) &\leq QIC(\Pi^1, \rho_1 \otimes \dots \otimes \rho_n) + QIC(\Pi^2, \sigma_1 \otimes \dots \otimes \sigma_m) \\ &= QIC(\Pi_2, \rho_1 \otimes \dots \otimes \rho_n \otimes \sigma_1 \otimes \dots \otimes \sigma_m) \\ &\leq QIC_{\otimes}(T_1 \otimes T_2) + \varepsilon'. \end{aligned}$$

Keeping tracks of rounds, we also get the bounded round result. ■

If we now consider  $n$ -fold product quantum task  $(\mathcal{N}, \rho, \varepsilon)^{\otimes n}$  and compare to the notation introduced when discussing amortized communication, we have  $\mathcal{T}_n(\mathcal{N}^{\otimes n}, \rho^{\otimes n}, \varepsilon) = \mathcal{T}_{\otimes}((\mathcal{N}, \rho, \varepsilon)^{\otimes n})$ . Correspondingly, we define

$$QIC_n(\mathcal{N}^{\otimes n}, \rho_n^{\otimes n}, \varepsilon) = QIC_{\otimes}((\mathcal{N}, \rho, \varepsilon)^{\otimes n}), \quad (6.5)$$

and the bounded round variant

$$QIC_n^M(\mathcal{N}^{\otimes n}, \rho_n^{\otimes n}, \varepsilon) = QIC_{\otimes}^M((\mathcal{N}, \rho, \varepsilon)^{\otimes n}). \quad (6.6)$$

Then we get by induction on the previous corollary the additivity result used in the proof of Theorem 2.

**Corollary 3** *For any quantum task  $(\mathcal{N}, \rho, \varepsilon)$  and bound  $M \in \mathbb{N}$  on the number of messages,*

$$\begin{aligned} nQIC(\mathcal{N}, \rho, \varepsilon) &= QIC_n(\mathcal{N}^{\otimes n}, \rho^{\otimes n}, \varepsilon), \\ nQIC^M(\mathcal{N}, \rho, \varepsilon) &= QIC_n^M(\mathcal{N}^{\otimes n}, \rho^{\otimes n}, \varepsilon). \end{aligned}$$

By definition and by using Lemma 1, we also get the following.

**Corollary 4** *For any quantum task  $(\mathcal{N}, \rho, \varepsilon)$  and bound  $M \in \mathbb{N}$  on the number of messages,*

$$\begin{aligned} QIC_n(\mathcal{N}^{\otimes n}, \rho^{\otimes n}, \varepsilon) &\leq QCC_n(\mathcal{N}^{\otimes n}, \rho^{\otimes n}, \varepsilon), \\ QIC_n^M(\mathcal{N}^{\otimes n}, \rho^{\otimes n}, \varepsilon) &\leq QCC_n^M(\mathcal{N}^{\otimes n}, \rho^{\otimes n}, \varepsilon). \end{aligned}$$

## 6.4 Convexity, Concavity and Continuity

We show that quantum information complexity is jointly convex in the channel and the error parameter. We also state the corollary that it is continuous in the error parameter, a fact used in the direct coding part of Theorem 2. Finally, we prove that the quantum information cost is concave in the input state.

We start with convexity.

**Lemma 5** *For any  $p \in [0, 1]$ , any two protocols  $\Pi^1, \Pi^2$  with  $M_1, M_2$  messages, respectively, there exists a  $M$ -message protocol  $\Pi$  satisfying  $\Pi = p\Pi^1 + (1 - p)\Pi^2$ ,  $M = \max(M_1, M_2)$ , such that the following holds for any state  $\rho$ :*

$$QIC(\Pi, \rho) = pQIC(\Pi^1, \rho) + (1 - p)QIC(\Pi^2, \rho).$$

**Proof.** Given  $\Pi^1, \Pi^2$ , we assume without loss of generality that  $M_1 \geq M_2$ , and we define  $\Pi$  in the following way:

---

Protocol  $\Pi$  on input  $\rho$ :

-The entangled state  $\psi$  contains many parts: it contains both entangled states  $\psi_1, \psi_2$  for the corresponding protocols  $\Pi^1, \Pi^2$ , it contains selector registers in state  $|\sigma_p\rangle = \sqrt{p}|1\rangle^{S_A}|1\rangle^{S_B} + \sqrt{1-p}|2\rangle^{S_A}|2\rangle^{S_B}$ , and it contains padding pure states to feed as input to

the protocol that is not selected, held in registers  $D_A, D_B$ .

-Coherently control what to input into the two protocols: on control set to 1, input state  $\rho$  into protocol  $\Pi^1$  and the padding pure state into protocol  $\Pi^2$ , and vice-versa on control set to 2.

-Run protocols  $\Pi^1, \Pi^2$  in parallel for  $M_2$  messages on given input until  $\Pi^2$  has finished.

-Finish running protocol  $\Pi^1$ .

-Coherently control what to output: on control set to 1, take as output the  $A_{out}, B_{out}$  registers of protocol  $\Pi^1$ , and on control set to 2, take those of protocol  $\Pi^2$ .

---

Note that by the structure of the above protocol and because the selector registers are traced out at the end, the output is of the form  $\Pi(\rho) = p\Pi^1(\rho) + (1 - p)\Pi^2(\rho)$ , and  $\Pi$  is a  $M$ -message protocol. We must now verify that the quantum information cost satisfies the stated property. First note that if Alice's registers are traced out, then Bob's selector register is effectively a classical register, and similarly for Alice's selector register if Bob's registers are traced out. Also note that throughout the protocol, due to the structure of  $\Pi$ , conditional on some classical state of the selector register, the reference register  $R$  can only be correlated with registers in the corresponding protocol, and  $D_B$  either contains a padding pure state or the input, with the later only when a padding pure state was input into  $\Pi$ . Also, still conditional on some classical state of the selector register, any register corresponding to  $\Pi^1$  is in product form with any register corresponding to  $\Pi^2$ . Then

$$\begin{aligned}
QIC(\Pi, \rho) &= I(C_1^1 C_1^2; R | B_{in} D_B T_B^1 T_B^2 S_B) + I(C_2^1 C_2^2; R | A_1^1 A_1^2 S_A) \\
&\quad + \cdots + I(C_{M_2}^1 C_{M_2}^2; R | A_{M_2-1}^1 A_{M_2-1}^2 S_A) \\
&\quad + I(C_{M_2+1}^1; R | B_{M_2}^1 B_{out}^2 (B')^2 S_B) + \cdots + I(C_{M_1}^1; R | A_{M_1-1}^1 A_{out}^2 (A')^2 S_A) \\
&= p(I(C_1^1 C_1^2; R | B_{in} D_B T_B^1 T_B^2 (S_B = 1)) + I(C_2^1 C_2^2; R | A_1^1 A_1^2 (S_A = 1))) \\
&\quad + \cdots + I(C_{M_2}^1 C_{M_2}^2; R | A_{M_2-1}^1 A_{M_2-1}^2 (S_A = 1)) \\
&\quad + I(C_{M_2+1}^1; R | B_{M_2}^1 B_{out}^2 (B')^2 (S_B = 1)) + \cdots + I(C_{M_1}^1; R | A_{M_1-1}^1 A_{out}^2 (A')^2 (S_A = 1))) \\
&\quad + (1 - p)(I(C_1^1 C_1^2; R | B_{in} D_B T_B^1 T_B^2 (S_B = 2)) + I(C_2^1 C_2^2; R | A_1^1 A_1^2 (S_A = 2))) \\
&\quad + \cdots + I(C_{M_2}^1 C_{M_2}^2; R | A_{M_2-1}^1 A_{M_2-1}^2 (S_A = 2)) \\
&\quad + I(C_{M_2+1}^1; R | B_{M_2}^1 B_{out}^2 (B')^2 (S_B = 2)) + \cdots + I(C_{M_1}^1; R | A_{M_1-1}^1 A_{out}^2 (A')^2 (S_A = 2))) \\
&= p(I(C_1^1; R | B_{in}^1 T_B^1 (S_B = 1)) + I(C_2^1; R | A_1^1 (S_A = 1)) + \cdots + I(C_{M_1}^1; R | A_{M_1-1}^1 (S_A = 1))) \\
&\quad + (1 - p)(I(C_1^2; R | B_{in}^2 T_B^2 (S_B = 2)) + I(C_2^2; R | A_1^2 (S_A = 2)) + \cdots) \\
&= pQIC(\Pi^1, \rho) + (1 - p)QIC(\Pi^2, \rho).
\end{aligned}$$

The first equality is by definition of quantum information cost of  $\Pi$ , and due to its parallel structure, the second equality uses the above remark about the selector register of one party being classical when the registers of the other party are traced out, along with a convex rewriting of conditional mutual information, the third equality uses the above remark about the product structure of  $R$  and the registers corresponding to  $\Pi^1, \Pi^2$ , respectively, depending on the classical state of the selector register, and the last equality is due to the fact that conditional on some classical state of the selector register, the state in the registers considered is the same as the one in the corresponding protocol. ■

We get the convexity in the channel and error parameters as a corollary.

**Corollary 5** For any  $p \in [0, 1]$ , define  $\mathcal{N} = p\mathcal{N}_1 + (1 - p)\mathcal{N}_2$  for any two channels  $\mathcal{N}_1, \mathcal{N}_2, \varepsilon = p\varepsilon_1 + (1 - p)\varepsilon_2$  for any two error parameters  $\varepsilon_1, \varepsilon_2 \in [0, 2]$ , for any bound  $M = \max(M_1, M_2)$ ,  $M_1, M_2 \in \mathbb{N}$  on the number of messages and for any input state  $\rho$ , the following holds:

$$\begin{aligned} QIC(\mathcal{N}, \rho, \varepsilon) &\leq pQIC(\mathcal{N}_1, \rho, \varepsilon_1) + (1 - p)QIC(\mathcal{N}_2, \rho, \varepsilon_2), \\ QIC^M(\mathcal{N}, \rho, \varepsilon) &\leq pQIC^{M_1}(\mathcal{N}_1, \rho, \varepsilon_1) + (1 - p)QIC^{M_2}(\mathcal{N}_2, \rho, \varepsilon_2). \end{aligned}$$

**Proof.** Let  $\Pi^1$  and  $\Pi^2$  be protocols satisfying, for  $i \in \{1, 2\}$ ,  $\Pi^i \in \mathcal{T}(\mathcal{N}_i, \rho, \varepsilon_i)$ ,  $QIC(\Pi^i, \rho) \leq QIC(\mathcal{N}_i, \rho, \varepsilon_i) + \delta$  for an arbitrary small  $\delta > 0$ , and take the corresponding protocol  $\Pi$  of Lemma 5. We first verify that protocol  $\Pi$  successfully accomplish its task. The result follows from the triangle inequality for the trace distance:

$$\begin{aligned} \|\Pi(\rho) - \mathcal{N}(\rho)\|_{A_{out}B_{out}R} &= \|p\Pi^1(\rho) + (1 - p)\Pi^2(\rho) - (p\mathcal{N}_1 + (1 - p)\mathcal{N}_2)(\rho)\|_{A_{out}B_{out}R} \\ &\leq \|p\Pi^1(\rho) - p\mathcal{N}_1(\rho)\|_{A_{out}B_{out}R} \\ &\quad + \|(1 - p)\Pi^2(\rho) - (1 - p)\mathcal{N}_2(\rho)\|_{A_{out}B_{out}R} \\ &\leq p\varepsilon_1 + (1 - p)\varepsilon_2 \\ &= \varepsilon. \end{aligned}$$

We must now verify that the quantum information cost satisfies the convexity property:

$$\begin{aligned} QIC(\mathcal{N}, \rho, \varepsilon) &\leq QIC(\Pi, \rho) \\ &= pQIC(\Pi^1, \rho) + (1 - p)QIC(\Pi^2, \rho) \\ &\leq pQIC(\mathcal{N}_1, \rho, \varepsilon_1) + (1 - p)QIC(\mathcal{N}_2, \rho, \varepsilon_2) + 2\delta. \end{aligned}$$

Keeping track of rounds, we get the bounded round result. ■

We get as a corollary that quantum information complexity is continuous in its error parameter. Note that quantum information complexity is decreasing in the error parameter.

**Corollary 6** For any  $\mathcal{N}, \rho, \varepsilon \in (0, 2], \delta > 0, M \in \mathbb{N}$ , there exists an  $0 < \varepsilon' < \varepsilon$  such that the following holds:

$$\begin{aligned} 0 &\leq QIC(\mathcal{N}, \rho, \varepsilon - \varepsilon') - QIC(\mathcal{N}, \rho, \varepsilon) \leq \delta, \\ 0 &\leq QIC^M(\mathcal{N}, \rho, \varepsilon - \varepsilon') - QIC^M(\mathcal{N}, \rho, \varepsilon) \leq \delta. \end{aligned}$$

We now show that quantum information is concave in its input state parameter.

**Lemma 6** For any  $p \in [0, 1]$ , define  $\rho = p\rho_1 + (1 - p)\rho_2$  for any two input states  $\rho_1, \rho_2$ . Then the following holds for any protocol  $\Pi$ :

$$QIC(\Pi, \rho) \geq pQIC(\Pi, \rho_1) + (1 - p)QIC(\Pi, \rho_2).$$

**Proof.** Consider purifications  $\rho_i^{A_{in}B_{in}R}$  of each  $\rho_i$ . By introducing a new selector reference subsystem  $S$ , we have the purification  $|\rho\rangle^{A_{in}B_{in}RS} = \sqrt{p}|\rho_1\rangle^{A_{in}B_{in}R}|1\rangle^S + \sqrt{1 - p}|\rho_2\rangle^{A_{in}B_{in}R}|2\rangle^S$ . Also consider the state  $\hat{\rho}^{A_{in}B_{in}R\hat{S}} =$



$\Delta_S(\rho^{A_{in}B_{in}RS})$  obtained if the  $S$  selector system was passed through a measurement channel  $\Delta^{S \rightarrow \hat{S}}$  to obtain classical system  $\hat{S}$ . We must verify that the quantum information cost satisfies the concavity property. We consider information quantities taken with respect to the protocol  $\Pi$  run on different inputs:  $\rho^{A_{in}B_{in}RS}, \hat{\rho}^{A_{in}B_{in}R\hat{S}}, \rho_2^{A_{in}B_{in}R}, \rho_2^{A_{in}B_{in}\hat{R}}$ , and identify with respect to which state we are considering by a subscript on the corresponding conditional mutual informations.

$$\begin{aligned}
QIC(\Pi, \rho) &= I(C_1; RS|B_0)_\rho + I(C_2; RS|A_1)_\rho + \dots \\
&\geq I(C_1; R\hat{S}|B_0)_{\hat{\rho}} + I(C_2; R\hat{S}|A_1)_{\hat{\rho}} + \dots \\
&= I(C_1; \hat{S}|B_0)_{\hat{\rho}} + I(C_1; R|\hat{S}B_0)_{\hat{\rho}} + I(C_2; \hat{S}|A_1)_{\hat{\rho}} + I(C_2; R|\hat{S}A_1)_{\hat{\rho}} + \dots \\
&\geq I(C_1; R|\hat{S}B_0)_{\hat{\rho}} + I(C_2; R|\hat{S}A_1)_{\hat{\rho}} + \dots \\
&= p(I(C_1; R|B_0)_{\rho_1} + I(C_2; R|A_1)_{\rho_1} + \dots) \\
&\quad + (1-p)(I(C_1; R|B_0)_{\rho_2} + I(C_2; R|A_1)_{\rho_2} + \dots) \\
&= pQIC(\Pi, \rho_1) + (1-p)QIC(\Pi, \rho_2).
\end{aligned}$$

The first equality is by definition of quantum communication cost of  $\Pi$  on input  $\rho$ , the first inequality uses the data processing inequality for conditional mutual information, the second equality is by the chain rule for conditional mutual information, the second inequality is by non-negativity of conditional mutual information, the third equality uses a convex rewriting of conditional mutual information, and the last equality is from definition. ■

## 6.5 Proof of Theorem 2

We now have all the tools to prove Theorem 2, that states that for any channel  $\mathcal{N}$ , any input state  $\rho$  and any error parameter  $\varepsilon \in (0, 2]$ ,  $QIC(\mathcal{N}, \rho, \varepsilon) = AQCC(\mathcal{N}, \rho, \varepsilon)$ . At  $\varepsilon = 2$ , both quantities vanish. The interesting regime is for  $\varepsilon \in (0, 2)$ . Note that keeping track of rounds, we get the result for bounded rounds.

For the direct coding part, to prove the  $\geq$  direction, we take an arbitrarily small  $\delta > 0$ , and use Corollary 6 to find an  $0 < \varepsilon' < \varepsilon$  such that  $QIC(\mathcal{N}, \rho, \varepsilon - \varepsilon') \leq QIC(\mathcal{N}, \rho, \varepsilon) + \delta$ . We then consider a protocol  $\Pi \in \mathcal{T}(\mathcal{N}, \rho, \varepsilon - \varepsilon')$  satisfying  $QIC(\Pi, \rho) \leq QIC(\mathcal{N}, \rho, \varepsilon - \varepsilon') + \delta$ . We now use Lemma 2 to find, for any sufficiently large  $n$ , a protocol  $\Pi_n \in \mathcal{T}(\Pi^{\otimes n}, \rho^{\otimes n}, \varepsilon')$  satisfying  $\frac{1}{n}QCC(\Pi_n) \leq QIC(\Pi, \rho) + \delta$ . We then have the following chain of inequality:

$$\begin{aligned}
\frac{1}{n}QCC(\Pi_n) &\leq QIC(\Pi, \rho) + \delta \\
&\leq QIC(\mathcal{N}, \rho, \varepsilon - \varepsilon') + 2\delta \\
&\leq QIC(\mathcal{N}, \rho, \varepsilon) + 3\delta.
\end{aligned}$$

Since  $\delta > 0$  is arbitrarily small and this holds for all sufficiently large  $n$ , we only have to verify that  $\Pi_n \in \mathcal{T}_n(\mathcal{N}^{\otimes}, \rho^{\otimes n}, \varepsilon)$  to complete the proof of the  $\geq$  direction. We have for each

$i \in [n]$ ,

$$\begin{aligned}
\|\text{Tr}_{\neg A_{out}^i B_{out}^i} \Pi_n(\rho^{\otimes n}) - \mathcal{N}(\rho)\| &\leq \|\text{Tr}_{\neg A_{out}^i B_{out}^i} \Pi_n(\rho^{\otimes n}) - \Pi(\rho)\| \\
&\quad + \|\Pi(\rho) - \mathcal{N}(\rho)\| \\
&\leq \|\Pi_n(\rho^{\otimes n}) - \Pi^{\otimes n}(\rho^{\otimes n})\| + \varepsilon - \varepsilon' \\
&\leq \varepsilon,
\end{aligned}$$

in which we first use the triangle inequality, and then monotonicity of the trace distance under partial trace.

For the converse part, to prove the  $\leq$  direction, we combine Corollary 3 and Corollary 4, and get the result since the following holds for all  $n$ :

$$\begin{aligned}
QIC(\mathcal{N}, \rho, \varepsilon) &= \frac{1}{n} QIC_n(\mathcal{N}^{\otimes n}, \rho^{\otimes n}, \varepsilon) \\
&\leq \frac{1}{n} QCC_n(\mathcal{N}^{\otimes n}, \rho^{\otimes n}, \varepsilon).
\end{aligned}$$

## 7 Quantum Information Complexity of Functions

### 7.1 Error for Classical Functions and Inputs

A potential application of the quantum information complexity paradigm is to prove quantum communication complexity lower bounds for classical functions. Hence, we want to make sure that the notion of distance we use for quantum channels and states is also an interesting one in such context. First, remember that for classical states  $\rho^{AB} = \sum_{x,y} p_{XY}(x,y) |x\rangle\langle x|^A \otimes |y\rangle\langle y|^B$ , we can use a canonical basis  $\{|xy\rangle\}$  to obtain a purification  $|\rho\rangle^{ABR} = \sum_{x,y} \sqrt{p_{XY}(x,y)} |x\rangle^A |y\rangle^B |xy\rangle^R$ . Then, for  $\Delta_R$  the measurement channel in the  $|xy\rangle$  basis on system  $R$ , we have

$$\|(\Pi \otimes \Delta_R)(\rho) - (\mathcal{N} \otimes \Delta_R)(\rho)\|_{ABR} \leq \|\Pi(\rho) - \mathcal{N}(\rho)\|_{ABR}$$

by the monotonicity of the trace distance under noisy channels. For classical functions, we consider channels  $\mathcal{N}$  such that we have

$$\mathcal{N}(|x\rangle\langle x|^{A_{in}} \otimes |y\rangle\langle y|^{B_{in}}) = |f_A(x,y)\rangle\langle f_A(x,y)|^{A_{out}} \otimes |f_B(x,y)\rangle\langle f_B(x,y)|^{B_{out}} \quad (7.1)$$

and then on classical inputs we have

$$(\mathcal{N} \otimes \Delta_R)(\rho^{ABR}) = \sum_{x,y} p_{XY}(x,y) |f_A(x,y)\rangle\langle f_A(x,y)|^{A_{out}} \otimes |f_B(x,y)\rangle\langle f_B(x,y)|^{B_{out}} \otimes |xy\rangle\langle xy|^R. \quad (7.2)$$

We get

$$\begin{aligned}
& \|(\Pi \otimes \Delta_R)(\rho) - (\mathcal{N} \otimes \Delta_R)(\rho)\|_{A_{out} B_{out} R} \\
&= \left\| \sum_{x,y} p_{XY}(x,y) |xy\rangle\langle xy|^R \otimes (\Pi(|x\rangle\langle x| \otimes |y\rangle\langle y|) \right. \\
&\quad \left. - |f_A(x,y)\rangle\langle f_A(x,y)| \otimes |f_B(x,y)\rangle\langle f_B(x,y)|) \right\|_{A_{out} B_{out} R} \\
&= \sum_{x,y} p_{XY}(x,y) \left\| \Pi(|x\rangle\langle x| \otimes |y\rangle\langle y|) \right. \\
&\quad \left. - |f_A(x,y)\rangle\langle f_A(x,y)| \otimes |f_B(x,y)\rangle\langle f_B(x,y)| \right\|_{A_{out} B_{out}},
\end{aligned}$$

so if we further apply the measurement channel  $\Delta_{AB}$  in the output basis,

$$\begin{aligned}
& \|(\Delta_{AB} \circ \Pi \otimes \Delta_R)(\rho) - (\Delta_{AB} \circ \mathcal{N} \otimes \Delta_R)(\rho)\|_{A_{out} B_{out} R} \\
&= \sum_{x,y} p_{XY}(x,y) \left\| \sum_{z_A, z_B} p_{Z_A Z_B | \Pi(x,y)}(z_A, z_B | \Pi(x,y)) |z_A\rangle\langle z_A| \otimes |z_B\rangle\langle z_B| \right. \\
&\quad \left. - |f_A(x,y)\rangle\langle f_A(x,y)| \otimes |f_B(x,y)\rangle\langle f_B(x,y)| \right\|_{A_{out} B_{out}} \\
&= \sum_{x,y} p_{XY}(x,y) ((1 - p_{Z_A Z_B | \Pi(x,y)}(z_A = f_A(x,y), z_B = f_B(x,y) | \Pi(x,y))) \\
&\quad + \sum_{(z_A, z_B) \neq (f_A(x,y), f_B(x,y))} p_{Z_A Z_B | \Pi(x,y)}(z_A, z_B | \Pi(x,y))) \\
&= \sum_{x,y} p_{XY}(x,y) (2Pr[\Delta_{AB} \circ \Pi(x,y) \neq (f_A(x,y), f_B(x,y))]),
\end{aligned}$$

and so applying monotonicity of the trace distance one last time, we get the following result.

**Lemma 7** *For classical functions  $f_A, f_B$ , a channel  $\mathcal{N}(|x\rangle\langle x| \otimes |y\rangle\langle y|) = |f_A(x,y)\rangle\langle f_A(x,y)| \otimes |f_B(x,y)\rangle\langle f_B(x,y)|$  and a classical input state  $\rho^{A_{in} B_{in}} = \sum_{x,y} p_{XY}(x,y) |x\rangle\langle x|^A \otimes |y\rangle\langle y|^B$ , the following holds for any  $\Pi(\mathcal{N}, \rho, \varepsilon)$ :*

$$\sum_{x,y} p_{XY}(x,y) (Pr[\Delta_{AB} \circ \Pi(x,y) \neq (f_A(x,y), f_B(x,y))]) \leq \frac{\varepsilon}{2}$$

## 7.2 Reduction of Disjointness to AND

In this section, we would like to establish a relationship between the quantum information cost of protocols computing the disjointness function and those computing the AND of two bits. The disjointness function is defined as  $DISJ_n(x, y) = \neg(\bigvee_{i \in [n]} x_i \wedge y_i)$ , for bit strings  $x = x_1 \cdots x_n, y = y_1 \cdots y_n$  and  $x_i \wedge y_i$  the AND of the two bits  $x_i, y_i$ . Given any protocol  $\Pi_D$  computing  $DISJ_n$  with error at most  $\varepsilon$  on all  $n$ -bit input, we can also use it to compute AND with error at most  $\varepsilon$  on all single bit input by setting  $n - 1$  inputs to 0 on one side. Consider any distribution  $\mu$  on 00, 01, 10, and the corresponding state  $\sigma_\mu = \mu(00)|00\rangle\langle 00| + \mu(01)|01\rangle\langle 01| + \mu(10)|10\rangle\langle 10|$ . We define in this way  $n$  different protocols  $\Pi_i$  for AND on an arbitrary input  $\rho$ , by setting, for  $i \in [n]$ , the  $i$ -th input to  $\Pi_D$  to the input

$\rho$  of the AND instance, and the  $n - 1$  remaining inputs to  $\sigma_\mu^{\otimes n-1}$ . We further combine them in a protocol  $\Pi_A$  that is their average. Running the average protocol on input  $\sigma_\mu$ , we get the following result.

**Theorem 4** *For any  $M$ -message protocol  $\Pi_D$  computing  $DISJ_n$  with error  $\varepsilon \in [0, 2]$  on all inputs, there exists a  $M$ -message protocol  $\Pi_A$  computing AND with error  $\varepsilon$  on all inputs and satisfying the following:*

$$QIC(\Pi_A, \sigma_\mu) = \frac{1}{n} QIC(\Pi_D, \sigma_\mu^{\otimes n}),$$

for the state  $\sigma_\mu = \mu(00)|00\rangle\langle 00| + \mu(01)|01\rangle\langle 01| + \mu(10)|10\rangle\langle 10|$ , and any probability distribution  $\mu$  on  $\{00, 01, 10\}$ .

**Proof.**

We first notice that we can replace the quantum criteria of error by the classical one for worst case input and obtain the same result. We fix  $\mu$  and simply write  $\sigma$  instead of  $\sigma_\mu$ . We start by defining the  $n$  protocols  $\Pi_i$  discussed above, and then use them to define the average protocol  $\Pi_A$ .

---

Protocol  $\Pi_i$  on input  $\rho$ :

- Let  $\psi_D$  be the entangled state used in  $\Pi_D$ , and consider a purification  $\sigma_j^{A_{in}^j B_{in}^j R^j}$  to  $\sigma_j$ , the  $j$ -th  $\sigma$  input to  $\Pi_D$ . The entangled state for the protocol will be  $\psi_D \otimes \sigma^{\otimes n-1}$ , with  $\sigma$ 's for all  $j$  different than  $i$ . The registers  $T_A, A_{in}^1, \dots, A_{in}^{i-1}, A_{in}^{i+1}, \dots, A_{in}^n, R^1, \dots, R^{i-1}$  are given to Alice, and  $T_B, B_{in}^1, \dots, B_{in}^{i-1}, B_{in}^{i+1}, \dots, B_{in}^n, R^{i+1}, \dots, R^n$  to Bob.
  - Using the  $\sigma_j$  states given as pre-shared entanglement to simulate the other inputs, run protocol  $\Pi_D$  on input  $\sigma_1 \otimes \dots \otimes \sigma_{i-1} \otimes \rho \otimes \sigma_{i+1} \otimes \dots \otimes \sigma_n$ .
  - Take as output the  $A_{out}, B_{out}$  registers of protocol  $\Pi_D$ .
- 

From these protocols, we define a new one for AND that is their uniform average.

---

Protocol  $\Pi_A$  on input  $\rho$ :

- The entangled state  $\psi_A$  contains many parts: it contains the  $\psi_D^{T_A T_B}$  entangled state for  $\Pi_D$ , as well as  $2n$   $\sigma$  states, with the  $R^j$  register given to Alice for the first  $n$  of them, and the  $R^j$  register given to Bob for the  $n$  last. Denote  $D_A = A_{in}^1 \otimes \dots \otimes A_{in}^{2n} \otimes R^1 \otimes \dots \otimes R^n$ ,  $D_B = B_{in}^1 \otimes \dots \otimes B_{in}^{2n} \otimes R^{n+1} \otimes \dots \otimes R^{2n}$  that correspond to Alice's and Bob's share of these states, respectively. The entangled state also contains some padding pure states  $\phi^{A_{in}^{\otimes(n-1)} B_{in}^{\otimes(n-1)}}$  to be swapped with the selected  $\sigma$ 's, held in registers  $P_A, P_B$ , and it also contains selector registers in state  $|\theta\rangle = \sum_i \frac{1}{\sqrt{n}} |i\rangle^{S_A} |i\rangle^{S_B}$ .
  - Coherently control what to input into the  $\Pi_D$  protocol: on control set to  $i$ , input state  $\rho$  into registers  $A_{in}^i B_{in}^i$ , use  $\sigma_1, \dots, \sigma_{i-1}$  in registers  $A_{in}^j B_{in}^j$  for  $j < i$ , and use  $\sigma_{n+i+1}, \dots, \sigma_{2n}$  in registers  $A_{in}^j B_{in}^j$  for  $j > i$ . Swap the padding pure states in  $P_A, P_B$  into the  $D_A, D_B$  registers that are used as input to  $\Pi_D$ .
  - Run protocol  $\Pi_D$  on given inputs until it has finished.
  - Take as output the  $A_{out}, B_{out}$  registers of protocol  $\Pi_D$ .
-

We first verify that protocol  $\Pi_A$  successfully accomplish its task. It is clear that each  $\Pi_i$  as well as  $\Pi_A$  are also  $M$  messages protocols. Note that by the structure of the above protocol and because the selector registers are traced out at the end, the output is of the form  $\Pi_A(\rho) = \sum_i \frac{1}{n} \rho_{out}^i$  for  $\rho_{out}^i = \Pi_i(\rho)$  the output of protocol  $\Pi_i$ . Further, each  $\Pi_i$  satisfies  $\Pi_i(\rho) = \Pi_D(\sigma_1 \otimes \cdots \otimes \sigma_{i-1} \otimes \rho \otimes \sigma_{i+1} \cdots \otimes \sigma_n)$ . Then, the result follows from the triangle inequality for the trace distance and the structure of the different protocols and channels, using the completely classical channels  $\mathcal{N}_A = AND \circ \Delta_{A_{in}B_{in}}, \mathcal{N}_D = DISJ_n \circ \Delta_{A_{in}B_{in}}$  to ensure that indeed, for any classical input  $\rho$  and any  $i \in [n]$ ,  $\mathcal{N}_A(\rho) = \mathcal{N}_D(\sigma_1 \otimes \cdots \otimes \sigma_{i-1} \otimes \rho \otimes \sigma_{i+1} \cdots \otimes \sigma_n)$ :

$$\begin{aligned}
\|\Pi_A(\rho) - \mathcal{N}_A(\rho)\|_{A_{out}B_{out}R} &= \left\| \sum_i \frac{1}{n} \rho_{out}^i - \sum_i \frac{1}{n} \mathcal{N}_A(\rho) \right\|_{A_{out}B_{out}R} \\
&\leq \sum_i \frac{1}{n} \|\rho_{out}^i - \mathcal{N}_A(\rho)\|_{A_{out}B_{out}R} \\
&= \sum_i \frac{1}{n} \|\rho_{out}^i - \mathcal{N}_D(\sigma_1 \otimes \cdots \otimes \sigma_{i-1} \otimes \rho \otimes \sigma_{i+1} \cdots \otimes \sigma_n)\|_{A_{out}B_{out}R} \\
&\leq \sum_i \frac{1}{n} \varepsilon \\
&= \varepsilon.
\end{aligned}$$

With a classical error parameter, the result follows by a similar average argument. We must now verify that the quantum information cost satisfies the desired property on input  $\rho = \sigma$ . First, note that if Alice's registers are traced out, then Bob's selector register is effectively a classical register, and similarly for Alice's selector register if Bob's registers are traced out. Then, conditional on some classical state of the selector register, the protocol  $\Pi_A$  acts as the corresponding protocol  $\Pi_i$  running  $\Pi_D$  on input  $\sigma_1 \otimes \cdots \otimes \sigma_{i-1} \otimes \sigma \otimes \sigma_{n+i+1} \otimes \cdots \otimes \sigma_{2n}$ , and the other  $\sigma_j$ 's and  $\phi$  are left untouched, in product form to  $R$  and all  $C_i$  registers. Then if

we run  $\Pi_A$  on input  $\sigma$ ,  $A_{in}B_{in}R$  act as  $A_{in}^iB_{in}^iR^i$  in  $\Pi_D$  on input  $\sigma^{\otimes n}$ , so

$$\begin{aligned}
QIC(\Pi_A, \sigma) &= I(C_1; R|B_{in}T_BP_BD_BS_B) + I(C_2; R|A_1D_AS_A) + I(C_3; R|B_2D_BS_B) + \dots \\
&= \frac{1}{n}(I(C_1; R|B_{in}T_BP_BD_B(S_B = 1)) + I(C_2; R|A_1D_A(S_A = 1)) \\
&\quad + I(C_3; R|B_2D_B(S_B = 1)) + \dots \\
&\quad + \dots \\
&\quad + I(C_1; R|B_{in}T_BP_BD_B(S_B = n)) + I(C_2; R|A_1D_A(S_A = n)) \\
&\quad + I(C_3; R|B_2D_B(S_B = n)) + \dots) \\
&= \frac{1}{n}(I(C_1; R^1|B_{in}^1(B_{in}^2 \dots B_{in}^n)T_B(S_B = 1)) + I(C_2; R^1|A_1R^2 \dots R^n(S_A = 1)) \\
&\quad + I(C_3; R^1|B_2(S_B = 1)) + \dots \\
&\quad + \dots \\
&\quad + I(C_1; R^i|(B_{in}^1 \dots B_{in}^{i-1})B_{in}^i(B_{in}^{i+1} \dots B_{in}^n)T_BR^1 \dots R^{i-1}(S_B = i)) \\
&\quad + I(C_2; R^i|A_1R^{i+1} \dots R^n(S_A = i)) \\
&\quad + I(C_3; R^i|B_2R^1 \dots R^{i-1}(S_B = i)) + \dots) \\
&= \frac{1}{n}(I(C_1; R^1 \dots R^n|B_{in}^1 \dots B_{in}^nT_B) + I(C_2; R^1 \dots R^n|A_1) \\
&\quad + I(C_3; R^1 \dots R^n|B_2) + \dots) \\
&= \frac{1}{n}QIC(\Pi_D, \sigma^{\otimes n}).
\end{aligned}$$

The first equality is by definition of quantum information cost of  $\Pi^A$ , the second equality uses the above remark about the selector register of one party being classical when the registers of the other party are traced out, along with a convex rewriting of conditional mutual information, the third equality uses the above remark about the product structure of the untouched  $\sigma$ 's in  $D_A, D_B$ , and about  $A_{in}B_{in}R$  acting as  $A_{in}^iB_{in}^iR^i$  depending on the classical state of the selector register, along with both the facts that mutual information in product systems is zero, and that conditioning on a product system is useless, the next equality follows by noticing that these quantities are the same as those in  $\Pi_D$ , and by recursively applying the chain rule from top to bottom for odd  $C_i$  terms, and from bottom up for even  $C_i$  terms, and then the last equality is by definition of the quantum information cost of  $\Pi_D$ .

Then  $\inf_{\Pi_A \in \mathcal{T}^M(AND, \varepsilon)} QIC(\Pi_A, \sigma_\mu) \leq \frac{1}{n} \inf_{\Pi_D \in \mathcal{T}^M(DISJ_n, \varepsilon)} QIC(\Pi_D, \sigma_\mu^{\otimes n})$ , in which the infima are taken over  $M$ -message protocols with worst-case error  $\varepsilon$  for classical inputs, on the respective functions. Then, for any  $\mu$ ,  $\inf_{\Pi_D \in \mathcal{T}^M(DISJ_n, \varepsilon)} QIC(\Pi_D, \sigma_\mu^{\otimes n}) \leq QCC^M(DISJ_n, \varepsilon)$ , and a lower bound on  $\inf_{\Pi_A \in \mathcal{T}^M(AND, \varepsilon)} QIC(\Pi_A, \sigma_\mu)$ , for any distribution  $\mu$  on  $00, 01, 10$ , implies a lower bound on the quantum communication complexity of any  $M$ -message protocol  $\Pi_D$  computing  $DISJ_n$  with worst case error  $\varepsilon$ . Is there a  $\mu$  for which we can get an interesting lower bound for  $\inf_{\Pi_A \in \mathcal{T}^M(AND, \varepsilon)} QIC(\Pi_A, \sigma_\mu)$ ? In particular, note that this lower bound would need to have a dependence on the number of rounds, since there are known protocols for computing  $DISJ_n$  at communication cost  $O(\frac{n}{M} + M)$  for  $M$ -message protocols, and in particular letting  $M \in \theta(\sqrt{n})$  in these we get an optimal protocol of  $\Theta(\sqrt{n})$  [1]. Note

that similar techniques were used in [27], adapted from the classical result of [4], to obtain a lower bound of  $\Omega(\frac{n}{M^2} + M)$  for bounded round protocols. However, with their different notion of quantum information cost, they started with a result that we would restate as  $\inf_{\Pi_A \in \mathcal{T}^M(AND, \varepsilon)} QIC'(\Pi_A, \sigma_\mu) \leq \frac{M}{n} \inf_{\Pi_D \in \mathcal{T}^M(DISJ_n, \varepsilon)} QCC(\Pi_D)$ , with the infima also taken with respect to  $M$ -message protocols. It is interesting to note that we seem to start with a factor of  $M$  less here. We suspect that the reason for this is the following. In our notation, their definition of their quantum information cost would be

$$QIC'(\Pi, \rho) = \sum_{i>0, odd} I(X; B_{i-1}|D) + \sum_{i>0, even} I(Y; A_{i-1}|D), \quad (7.3)$$

for protocols that keep local copies  $X, Y$  of Alice's and Bob's classical inputs, and in which it is requested of  $\mu$  that, for some random variable  $D$  inaccessible to Alice and Bob and conditional on the event  $D = d$ , the classical random variables  $X_d = X|(D = d), Y_d = Y|(D = d)$  are independent. Note that if we take the uniform distribution on Alice's input and the 0 input for Bob, a product distribution, then any protocol that starts by distributing copies of all of Alice's bit, and then simply exchange a dummy qubit in the  $|0\rangle$  state for all remaining messages, would have  $QIC' \in \Omega(M \cdot n)$ , for  $M$  messages and  $n$  bits inputs. The communication is of the order of  $M+n$ , so for  $M \in \omega(1)$ , since we are interested in the regime  $M \leq n$ , this is a factor of  $M$  more than the communication. In contrast to their notion, our definition of quantum information cost is bounded by the communication. If we could get a bound proportional to theirs for  $\inf_{\Pi_A \in \mathcal{T}^M(AND, \varepsilon)} QIC(\Pi_A, \sigma_\mu) \in \Omega(\frac{1}{M})$ , we would get a lower bound of  $\Omega(\max(M, \frac{n}{M}))$  on communication, thus matching the best known upper bound for bounded round quantum protocol for  $DISJ_n$ . We conjecture that this is the case, and so that this is worth looking into. Note however that this would probably require new techniques to lower bound the conditional quantum mutual information, a quantity which is notoriously hard to lower bound [30, 13]. We further discuss these issues in the conclusion.

## 8 Conclusion

We have defined a new notion of quantum information cost and a corresponding notion of quantum information complexity. In contrast to previously defined notions, these directly provide a lower bound on the communication, independent of round complexity. To define the quantum information cost of a protocol on an input quantum state, we take a detour through classical information cost and provide a different perspective on it, relating it to noisy channels simulation with side information at the receiver, a variant of the classical reverse Shannon theorem studied in information theory. This provides a different proof that the information complexity is an achievable rate for amortized communication complexity, one that preserves the round complexity, and leads to an easier quantum generalization than the transcript based view on classical information cost. Using this quantum generalization, we provide an operational interpretation for the  $\varepsilon$ -error quantum information complexity of a channel  $\mathcal{N}$  on input  $\rho$  as the  $\varepsilon$ -error amortized quantum communication complexity of  $\mathcal{N}$  on input  $\rho$ , and in this sense provides the right quantum generalization of the classical information complexity. We prove some interesting properties of quantum information complexity, like additivity and convexity. We also prove that on channels implementing, with  $\varepsilon$

error, through a protocol  $\Pi$ , a classical function  $f$  on a classical input distributed according to  $\mu$ , the error criterion that we use provides an upper bound on the average probability of failure,  $Pr_\mu[\Pi(x, y) \neq f(x, y)] \leq \frac{\varepsilon}{2}$ , hence giving it an operational meaning in the context of quantum information complexity of classical functions.

An important application of classical information complexity is to prove communication complexity lower bounds, and it is reasonable to hope that quantum information complexity will lead to interesting lower bound on quantum communication complexity. In [27], the authors use a different quantum generalization of information cost to derive an elegant proof of a lower bound on the bounded round quantum communication complexity of set disjointness. For  $M$ -message protocols, the authors prove a lower bound of  $\Omega(\frac{n}{M^2} + M)$  on the quantum communication complexity of  $DISJ_n$ , close to the best known upper bound of  $O(\frac{n}{M} + M)$ . However, the notion of quantum information cost that they use can be as high as  $\Omega(M \cdot C)$  for  $M$ -message protocols communicating  $C$  qubits. Could we use our notion of quantum information cost, which does not have this possible dependence on  $M$ , to close the gap and prove a lower bound of  $\Omega(\frac{n}{M} + M)$  on the quantum communication complexity? We are able to show that on  $(n$ -fold tensor) classical inputs with no support for  $x = y = 1$ , the quantum communication cost of any good protocol (with low error on all input) for  $DISJ_n$  is at least  $n$  times the quantum information cost for any good protocol for the AND function on the same input. In contrast, in [27] they obtain a bound of at least  $\frac{n}{M}$  times for a related quantity. However, we fall short of proving a  $\Omega(\frac{1}{M})$  lower bound on the quantum information cost of good protocols for the AND function. The reason for this is that, for the moment, we lack the necessary tools to lower bound the quantum information cost, which is defined as a sum of conditional mutual information with a quantum conditioning register. In [27] the conditioning system is classical, and conditioning on a classical system is equivalent to taking an average. They are then able, through a clever combination of a local transition lemma and an average encoding theorem, to relate the sum of the square roots of all terms in their quantum information cost quantity to the probability of success of the  $M$ -message protocol. The round dependent lower bound follows by using a convexity argument to put these terms inside the square root. Could we do something similar? The conditional quantum mutual information has an history of being hard to lower bound [30, 13], but hopefully recent developments in quantum information theory will help in this task. In particular, Berta, Seshadreesan and Wilde lists many rewriting of the conditional mutual information in terms of a divergence quantity [12]; hopefully it will be possible to use such a rewriting to derive an analogue of the average encoding theorem [29] with a quantum conditioning register. Note that the purifying register  $R$  can play the role of a classical system for us, since by the data processing inequality we can measure it first and still obtain a valid lower bound. Maybe another approach to lower bound quantum information complexity would be to try to extend to the quantum setting the powerful approach of Kerenidis, Laplante, Lerays and Roland through zero-error protocols [28]. Note that Chailloux and Scarpa define a notion of superposed information cost [20] appropriate for entangled games with no communication to obtain an exponential decay result for parallel repetition of such games. Is there a connexion between this quantity and ours?

We are confident that this new notion of quantum information complexity will stimulate interesting developments in quantum communication complexity, as well as in quantum information theory to obtain tools that would prove helpful for such developments. Inter-



esting directions for this research program is first to obtain interesting lower bound on the quantum information complexity of specific functions, possibly by developing further techniques for lower bounding the conditional mutual information. Also, with the operational interpretation that we prove for quantum information complexity, this opens the door to the study of direct sum questions in quantum communication complexity. A direct sum results shows that to implement  $n$  instances of a task requires something on the order of  $n$  times the resources needed to implement a single instance of the task. Hence, the ability to compress the best protocols down to something close to their quantum information cost would lead to a direct sum result. A first step in this direction could be to try to obtain such a single-copy compression result for bounded round protocols, possibly by using a one-shot version of the state redistribution protocol. However, the one-shot result of [37] does not seem to be sufficient for this purpose. Does there exist one-shot protocols for state redistribution, possibly interactive, that would enable us to obtain interesting compression results for the bounded round scenario? Note that a quantum generalisation of the correlated sampling protocol of Braverman and Rao [19] has been proved recently [3]. In this quantum version, if Alice knows the spectral decomposition of a state  $\rho$ , Bob knows the spectral decomposition of a state  $\sigma$ , and both know the relative entropy  $D(\rho||\sigma)$  between these, then using shared entanglement, Bob can sample a state  $\tilde{\rho}$  close to  $\rho$  at communication cost proportional to  $D(\rho||\sigma)$ . Can we further generalize this to a setting with quantum side information, to compress messages while keeping quantum correlation? Another interesting research direction would be to try to obtain the quantum analogue of the result about a prior-free information cost and its relation to worst-case amortized communication complexity. A first approach to try for this problem could be to obtain a composable quantum reverse Shannon theorem on arbitrary input, with feedback and side information at the receiver that would be tailor-made for our purpose. However, even in the case without side information at the receiver, it is known that for the arbitrary input case, standard entanglement, such as maximally entangled states, is not sufficient, and more exotic forms of entanglement such as entanglementembezzling states [23] are needed [8, 11]. As is made clear from our direct coding theorem, those reverse Shannon theorems achieve a stronger, global error parameter than the more local one that we require. Are these forms of entanglement also required in this restricted scenario?

Finally, it would be interesting to see if the quantum information complexity paradigm would enable to shed some light on the question of equivalence between the model of Yao versus the model of Cleve-Buhrman for quantum communication complexity. Our communication model is closer to the Cleve-Buhrman one, and we use the pre-shared entanglement in a crucial way in many of our results. It would be possible in principle, even though the interpretation might not be the same, to define the quantum information complexity in the Yao model by restricting the infimum to be taken over protocols where the state  $\psi$  is a pure product state. But since we can distribute entanglement at no cost with our definition of quantum information cost, what would be an appropriate definition in this setting? Would it be any easier to relate the information complexity in these two models than it is to relate the corresponding communication complexities? And what about amortized communication complexity?

**Acknowledgement** We are grateful to Omar Fawzi for a stimulating discussion in the early stages of this work and for useful feedback on a previous version, as well as to Gilles Brassard and Alain Tapp for useful discussions and feedback during the write-up of this paper. We acknowledge financial support from a Fonds de Recherche Québec-Nature et Technologies B2 Doctoral research scholarship.

## A External Information: Classical and Quantum

The material in this section is more exploratory in nature, and is still work in progress. Correspondingly, the presentation will be less formal, but ideas from the previous sections can be used to formalize the material here. It can safely be skipped without affecting understanding in the other sections.

The classical external information cost is defined as  $IC^{ext} = I(XY; \Pi(X, Y))$ , and is usually viewed as a measure of how much information the protocol leaks about the input to an external observer, being an allowed observer or a potential eavesdropper. It is a natural quantity to use for example in the standard communication complexity setting with cryptographic consideration, and also in the simultaneous message passing model, in which Alice and Bob must send simultaneously a single message to an external referee who must produce the output. We give two alternative interpretations of this quantity, one in the standard communication complexity setting, and one in a generalization of the simultaneous message passing model. We then show that the quantum generalizations give rise to two different quantities, even though they were both characterized by a unique classical quantity, and so the external information cost has a dual role depending on the interpretation we want to give it.

Let us first define the generalization of the simultaneous message passing model that we consider. We consider the same definition for classical protocols as given in section 4, but the difference is now in the output: instead of having as output of the protocol Alice and Bob outputting some function of the transcript and their local input, we now want to have an external referee  $R$  generating the output to the protocol by computing some function of the transcript only. If we want to obtain the simultaneous message model from this generalization, we restrict protocols to two messages, and require the following Markov condition:  $M_2|M_1YR = M_2|YR$ , i.e. the second message must be independent of the first message when conditioned on the input  $Y$  and shared randomness  $R$ .

The important point to notice is that now, when compressing the protocol, we must insure that the referee gets all the necessary information in the transcript. We define an alternate external information cost quantity as  $IC_\mu^{ext} = I(M_1^R; XR^A|R^R) + I(M_2^R; YM_1^B R^B|M_1^R R^R) + I(M_3^R; XM_2^A M_1^A R^A|M_2^R M_1^R R^R) + \dots + I(M_N^R; YM_{N-1}^B \dots M_1^B R^B|M_{N-1}^R \dots M_1^R R^R)$ , in which we distinguish between Alice's, Bob's and the referee's copy of the public randomness  $R$  and the messages  $M_i$ . Note that this is easily seen to be equivalent to  $IC^{ext}$ , using a similar argument as for the internal information cost, along with a combination of the chain rule and the Markov condition on messages versus the inputs:  $M_i|XYM_{i-1} \dots R = M_i|YM_{i-1} \dots R$  for even  $i$ , and  $M_i|XYM_{i-1} \dots R = M_i|XM_{i-1} \dots R$  for odd  $i$ . Similar to the case for internal information cost, the external information cost can then be viewed as an asymptotically achievable cost for transferring the messages such that both the other player and the referee

can get the information, in the limit of many protocols. We then get an operational interpretation for the external information complexity as an achievable amortized communication complexity in this setting with an external referee. It is then clear that the external information should be interesting in the simultaneous message passing model. Note that this setting in the interactive case is interesting only when the entropy of  $f$ , for  $f$  the output function, is much larger than the internal information complexity, since otherwise Alice and Bob can simply compute  $f$  at this cost and send the result to the referee at small additional cost.

It is less straightforward to generalize this to the quantum setting, mostly due to the fact that we cannot send a copy of messages to both the other player and to a referee in the quantum setting. The quantum generalization of this setting would be the following: given a quantum channel  $\mathcal{N} \in \mathcal{C}(A_{in} \otimes B_{in}, R_{out})$  and input state  $\rho \in \mathcal{D}(A_{in} \otimes B_{in})$ , Alice and Bob are given input register  $A_{in}, B_{in}$  at the outset of the protocol, respectively, and the referee should output register  $R_{out}$  at the end of the protocol, which should be in state  $\mathcal{N}(\rho)$  up to some small error. In the protocol, at each time step, after applying their unitary, the players send a communication register to the other player, and another one to the referee, and keep some quantum memory. They want to minimize the total communication cost, that is, the sum of the cost from player to referee, and from player to player. The players and the referee can share an arbitrary tripartite entangled state at the outset of the protocol. A reasonable external quantum information cost for this setting, with the operational interpretation of being an asymptotically achievable rate of total communication, would follow in the same way as the standard quantum information cost quantity, from repeated application of state redistribution, along with an appropriate partition of the side information and unavailable information in this setting.

If we instead want to take the eavesdropper view on the external information cost, we go back to the standard two-party communication complexity setting, and want to consider a passive eavesdropper, who has access to previous correlation, to all communication and to all garbage information from the protocol at the end (classically, this would be the transcript), but is not allowed to alter the communication. However, this quantity, when evaluated in a quantum setting for classical functions and inputs would be bounded by a constant due to the fact that a passive quantum eavesdropper cannot listen to the quantum communication, and due to the presence of reversible computing in the quantum world (see [14] for a discussion), which would limit the amount of information the passive eavesdropper would get at the end.

Note that this channel simulation view of information cost also leads rather straightforwardly to possibly interesting definitions of information cost in a multipartite setting, in particular in a model with some external coordinator, as an achievable rate of total asymptotic communication which lower bounds single-copy communication. It is then possible to define appropriate quantum generalizations, by carefully adapting the model, and then once again by considering repeated application of state redistribution. Of course, the interest of such information cost quantities find their interest in potential applications. We leave such possible applications of these potential definitions for future work.

## References

- [1] Scott Aaronson, and Andris Ambainis. *Quantum Search of Spatial Regions*. Proceedings of the 44rd Annual IEEE Symposium on Foundations of Computer Science (2003): 200-209.
- [2] Anura Abeyesinghe, Igor Devetak, Patrick Hayden, and Andreas Winter. *The mother of all protocols: Restructuring quantum information's family tree*. Proceedings of the Royal Society of London. Series A (2009): 2537-2563.
- [3] Anurag Anshu, Rahul Jain, Priyanka Mukhopadhyay, Ala Shayeghi, and Penghui Yao. *A new operational interpretation of relative entropy and trace distance between quantum states*. arXiv:quant-ph/1404.1366.
- [4] Ziv Bar-Yossef, T. S. Jayram, Ravi Kumar, and D. Sivakumar. *An information statistics approach to data stream and communication complexity*. Proceedings of the 43rd Annual IEEE Symposium on Foundations of Computer Science (2002): 209-218.
- [5] Boaz Barak, Mark Braverman, Xi Chen, and Anup Rao. *How to compress interactive communication*. Proceedings of the 42nd Annual ACM Symposium on Theory of Computing (2010): 67-76.
- [6] Howard Barnum, Claude Crepeau, Daniel Gottesman, Adam Smith, and Alain Tapp. *Authentication of Quantum Messages*. Proceedings of the 43rd Annual IEEE Symposium on Foundations of Computer Science (2002): 449-458.
- [7] Charles H. Bennett, Gilles Brassard, Claude Crépeau, Richard Jozsa, Asher Peres, and William K. Wootters. *Teleporting an unknown quantum state via dual classical and Einstein-Podolsky-Rosen channels*. Physical Review Letters 70.13 (1993): 1895-1899.
- [8] Charles H. Bennett, Igor Devetak, Aram W. Harrow, Peter W. Shor, and Andreas Winter. *Quantum Reverse Shannon Theorem*. arXiv:quant-ph/0912.5537.
- [9] Charles H. Bennett, Peter W. Shor, John A. Smolin, and Ashish V. Thapliyal. *Entanglement-assisted capacity of a quantum channel and the reverse Shannon theorem*. IEEE Transactions on Information Theory 48.10 (2002): 2637-2655.
- [10] Charles H. Bennett and Stephen J. Wiesner. *Communication via one- and two-particle operators on Einstein-Podolsky-Rosen states*. Physical Review Letters 69.20 (1992): 2881-2884.
- [11] Mario Berta, Matthias Christandl, Renato Renner. *The Quantum Reverse Shannon Theorem based on One-Shot Information Theory*. Communications in Mathematical Physics 306 (2011): 579-615.
- [12] Mario Berta, Kaushik Seshadreesan, and Mark M. Wilde. *Renyi generalizations of the conditional quantum mutual information*. arXiv:quant-ph/1403.6102.

- [13] Fernando G. S. L. Brandao, Matthias Christandl, Jon Yard. *Faithful Squashed Entanglement*. Communications in Mathematical Physics 306 (2011): 805-830.
- [14] Mark Braverman. *Interactive information complexity*. Proceedings of the 44th Annual ACM Symposium on Theory of Computing (2012): 505-524.
- [15] Mark Braverman. *Coding for Interactive Computation: Progress and Challenges*. Proceedings of the 50th Annual Allerton Conference on Communication, Control, and Computing (2012): 1914:1921.
- [16] Mark Braverman, Faith Ellen, Rotem Oshman, Toniann Pitassi, and Vinod Vaikanathan. *Tight bounds for set disjointness in the message passing model*. Proceedings of the 54th Annual IEEE Symposium on Foundations of Computer Science (2013): 668-677.
- [17] Mark Braverman, Ankit Garg, Denis Pankratov, and Omri Weinstein. *From information to exact communication*. Proceedings of the 45th Annual ACM Symposium on Theory of Computing (2013): 151-160.
- [18] Mark Braverman, and Ankur Moitra. *An information complexity approach to extended formulations*. Proceedings of the 45th Annual ACM Symposium on Theory of Computing (2013): 161-170.
- [19] Mark Braverman, and Anup Rao. *Information equals amortized communication*. Proceedings of the 52nd Annual IEEE Symposium on Foundations of Computer Science (2011): 748-757.
- [20] André Chailloux, and Giannicola Scarpa. *Parallel Repetition of Entangled Games with Exponential Decay via the Superposed Information Cost*. arXiv:quant-ph/1310.7787, presented at QIP2014.
- [21] Richard Cleve, and Harry Buhrman. *Substituting quantum entanglement for communication*. Physical Review A 56.2 (1997): 1201-1204.
- [22] A. Chakrabarti, Yaoyun Shi ; A. Wirth, Andrew C.-C. Yao. *Informational complexity and the direct sum problem for simultaneous message complexity*. Proceedings of the 42nd Annual IEEE Symposium on Foundations of Computer Science (2001): 270-278.
- [23] Wim van Dam, and Patrick Hayden. *Universal entanglement transformations without communication*. Physical Review A 67.6 (2003): 060302(R).
- [24] Igor Devetak, and Jon Yard. *Exact cost of redistributing multipartite quantum states*. Physical Review Letters 100.23 (2008): 230501.
- [25] Dennis Dieks. *Communication by EPR devices*. Physics Letters A 92.6 (1982):271-272.
- [26] Rahul Jain, and Ashwin Nayak. *The space complexity of recognizing well-parenthesized expressions in the streaming model: the Index function revisited*. arXiv: cs.cc/1004.3165.

- [27] Rahul Jain, Jaikumar Radhakrishnan, and Pranab Sen. *A lower bound for bounded round quantum communication complexity of set disjointness*. Proceedings of the 44th Annual IEEE Symposium on Foundations of Computer Science (2003): 220-229.
- [28] Iordanis Kerenidis, Sophie Laplante, Virginie Lerays, Jérémie Roland, and David Xiao. *Lower Bounds on Information Complexity via Zero-Communication Protocols and Applications*. Proceedings of the 53rd Annual IEEE Symposium on Foundations of Computer Science (2012): 500-509.
- [29] Hartmut Klauck, Ashwin Nayak, Amnon Ta-Shma, David Zuckerman. *Interaction in quantum communication and the complexity of set disjointness*. Proceedings of the 33rd Annual ACM Symposium on Theory of Computing (2001): 124-133.
- [30] Elliott H. Lieb, and Mary Beth Ruskai. *Proof of the strong subadditivity of quantum-mechanical entropy*. Journal of Mathematical Physics, 14 (1973): 1938-1941.
- [31] Zhicheng Luo, and Igor Devetak. *Channel Simulation With Quantum Side Information*. IEEE Transactions on Information Theory 55.3 (2009): 1331-1342.
- [32] Laura Mančinska, Thomas Vidick. *Unbounded entanglement can be needed to achieve the optimal success probability*. arXiv:quant-ph/1402.4145.
- [33] John Watrous. *Theory of Quantum Information*. Lecture notes from Fall 2013, <https://cs.uwaterloo.ca/~watrous/CS766/> (2013).
- [34] Mark M. Wilde. *Quantum Information Theory*. Cambridge University Press (2013), Preliminary version available as: arXiv e-print quant-ph/1106.1445.
- [35] William K. Wootters, and Wojciech H. Zurek. *A single quantum cannot be cloned*. Nature 299.5886 (1982): 802-803.
- [36] Andrew C.-C. Yao. *Quantum circuit complexity*. Proceedings of the 34th Annual IEEE Symposium on Foundations of Computer Science (1993): 352-361.
- [37] Jon T. Yard, and Igor Devetak. *Optimal Quantum Source Coding With Quantum Side Information at the Encoder and Decoder*. IEEE Transactions on Information Theory 55.11 (2009): 5339-5351.